INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Autarquia Associada à Universidade de São Paulo

Metodologia de especificação de sistemas de instrumentação e controle para usinas nucleares móveis

CLAUDIO SIQUEIRA SANTOS

Dissertação apresentada como parte dos requisitos para obtenção do Grau de Mestre em Ciências na Área de Tecnologia Nuclear - Reatores

Orientador:

Prof. Dr. Delvonei Alves de Andrade

São Paulo

2021

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Autarquia Associada à Universidade de São Paulo

Metodologia de especificação de sistemas de instrumentação e controle para usinas nucleares móveis

Versão Corrigida

Versão Original disponível no IPEN

CLAUDIO SIQUEIRA SANTOS

Dissertação apresentada como parte dos requisitos para obtenção do Grau de Mestre em Ciências na Área de Tecnologia Nuclear - Reatores

Orientador:

Prof. Dr. Delvonei Alves de Andrade

São Paulo

2021

Como citar:

SANTOS, C. S. ***Metodologia de especificação de sistemas de instrumentação e controle para usinas nucleares móveis***. 2021. 145 f. Dissertação (Mestrado em Tecnologia Nuclear) – Instituto de Pesquisas Energéticas e Nucleares, IPEN-CNEN/SP, São Paulo. Disponível em: ‹http://repositorio.ipen.br/› (data de consulta no formato: dd/mm/aaaa)

Ficha catalográfica elaborada pelo sistema de geração automática da Biblioteca IPEN/USP,
Com os dados fornecidos pelo autor.

Santos, Claudio Siqueira
Metodologia de especificação de sistemas de instrumentação e controle para usinas nucleares móveis / Claudio Siqueira Santos; orientador Delvonei Alves de Andrade. -- São Paulo, 2021.
145 f.

Dissertação (Mestrado) - Programa de Pós-Graduação em Tecnologia Nuclear (Reatores) -- Instituto de Pesquisas Energéticas e Nucleares, São Paulo, 2021.

1. Sistemas Instrumentação e Controle. 2. Arquitetura de sistemas nucleares. 3. Small Modular Reactor. 4. Usina Nuclear Móvel. 5. Guia para elaboração de análise funcional e de requisitos de sistemas . I. de Andrade, Delvonei Alves, orient. II. Título.

FOLHA DE APROVAÇÃO

Autor: CLAUDIO SIQUEIRA SANTOS

Título: Metodologia de especificação de sistemas de instrumentação e controle para usinas nucleares móveis

Dissertação apresentada como parte dos requisitos para obtenção do Grau de Mestre em Tecnologia Nuclear - Reatores.

Data:_22/11/2021

Banca Examinadora:

Prof. Dr. Delvonei Alves de Andrade

Instituição: IPEN/USP Julgamento: Aprovado

Prof. Dr. Paulo Fernando Ferreira Frutuoso e Melo

Instituição: UFRJ Julgamento: Aprovado

Prof. Dr. Luciano Ondir Freire

Instituição: Marinha Julgamento: Aprovado

Dedicatória

À minha esposa Izabela Azevedo do Nascimento, razão da minha vida. Gratidão eterna pela paciência e pelo apoio nestes anos de estudo. Aos meus filhos João Paulo Santos do Nascimento, Filipe Mariano Santos do Nascimento, Maria Isabel Santos do Nascimento e Tomás Santos do Nascimento, pelo carinho e atenção que sempre me deram nessa caminhada. E ao pequenino ser tão amado no ventre da minha esposa.

Agradecimentos

A Deus, fim único da minha existência. À Santíssima Virgem Mãe de Deus, a quem continuamente recorro para que me proteja.

Ao meu orientador, Prof. Dr. Delvonei Alves de Andrade, que me motivou continuamente, e me orientou com destreza necessária para a conclusão deste trabalho.

Ao Doutor Luciano Ondir Freire, cuja tese de doutorado no IPEN/USP foi guia para o desenvolvimento deste estudo. Grato pela grande contribuição nas consultas realizadas para retirada de dúvidas.

Aos meus pais Claudionor Castro Santos e Rosângela Siqueira Santos, que sempre me apoiaram em tudo na vida! Ao meu pai pelo exemplo de justiça e dedicação, pessoa em quem sempre me espelhei. E a minha mãe, pela delicadeza e carinho com que sempre me tratou e cuidou.

A toda a minha família, a quem dedico também essa conquista tão importante. Meu irmão Renato, sua esposa Paulyne e meus sobrinhos Antônio e Helena. Minha cunhada Juliana e seu marido Ricardo, e meu sobrinho Arthur. Aos meus sogros Pedro e Rosângela, fundamentais também por todo o apoio que sempre dispensaram.

Aos meus colegas de trabalho do CTMSP, que me oportunizou e me desafiou a esta aventura da pós-graduação. Gratidão enorme aos chefes diretos com quem trabalhei neste período e que sempre me apoiaram nesta empreitada, o Engenheiro João Manoel A. Carregado, Engenheiro João Carlos Mariano (*in memoriam*), CC (EN) Diego Francelino e CMG (RM-1-EN) Osvaldo Monteiro.

Aos meus amigos queridos do Grupo Famílias em Cristo, que sempre rezaram por mim. Aos Padres amigos e fiéis pais espirituais Matheus Pigozzo, Demétrio Gomes e Anderson Batista. Ao meu companheiro espiritual Luiz Eduardo Meira, a quem devo imenso agradecimento pelas orações.

Aos meus colegas de turma do programa, que tornaram a jornada mais leve com alegria e entusiasmo!

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001.

RESUMO

SANTOS, C. S. **Metodologia de especificação de sistemas de instrumentação e controle para usinas nucleares móveis**. 2021. 145p. Dissertação (Mestrado em Tecnologia Nuclear) – Instituto de Pesquisas Energéticas e Nucleares – IPEN-CNEN/SP. São Paulo.

Os Sistemas de Instrumentação e Controle (I&C) são responsáveis pela aquisição, tratamento, transmissão, conversão e controle de todos os sistemas de processo de uma Usina Nuclear Móvel (UNM). Por esta razão, os sistemas de I&C contribuem com a UNM, para que esta atinja os objetivos gerais de disponibilidade e confiabilidade, melhorando a segurança, reduzindo custos operacionais, além de incrementar a produtividade. O uso de tecnologias modernas de softwares e metodologias de projeto é a chave que contribuirá de sobremaneira na melhora competitiva em projetos de UNM e na redução dos custos de implementação de sistemas de I&C. Os números de um projeto de sistemas de I&C exigem um eficaz gerenciamento de dados no projeto, podendo chegar a 10.000 sensores e detectores, 5.000 quilômetros de cabos, e um total de 1.000 toneladas de massa. Além disso, a especificação de sistemas de I&C tem entradas e saídas multidisciplinares. As diferentes formações técnicas e acadêmicas dos atores envolvidos no projeto podem conduzir a divergências de opinião, e no processo decisório partirem para soluções de curto prazo. Desta forma, aumentam-se os riscos de atrasos no projeto, por conta de erros de especificações e atrasos na implementação e validação de *hardware* e *software* de controle. O objetivo principal deste trabalho é propor uma metodologia que clarifique os principais fluxos de dados no projeto básico de sistemas de I&C. O método proposto visa a aplicação de uma a estruturação de especificação "*top-down*", com foco na definição das funções de controle, requisitos, arquiteturas de I&C, gestão de interfaces, e que, além disso, garanta a aplicação da lei construtal na especificação destes sistemas. O resultado da metodologia é garantir que todos os atores envolvidos tenham uma visão global de toda análise funcional e da definição de requisitos desde o mais alto nível (da UNM) até os níveis inferiores (dos equipamentos), assegurando a passagem de fluxos de informações, garantindo a segurança, reduzindo prazos e custos no projeto.

Palavras-chave: Sistemas Instrumentação e Controle; Arquitetura de sistemas nucleares; Guia para elaboração de análise funcional e de requisitos de sistemas I&C; Reatores Modulares; Usina Nuclear Móvel.

ABSTRACT

SANTOS, C. S. **A Methodology for the specification of instrumentation and control systems for mobile nuclear power plants.** 2021. 145p. Dissertation (Master in Nuclear Technology) – Institute of Energy and Nuclear Research – IPEN-CNEN/SP. São Paulo.

The Instrumentation and Control systems (I&C systems) are responsible to acquire, to treat, to transmit, to convert, and to control every process systems in a Mobile Nuclear Power Plant (NPP). For this reason, I&C systems enhance the ability to achieve the goals of improved availability and reliability, enhanced safety, reduced operations and maintenance costs, and improved productivity in NPP. The use of modern technology of software and design methodologies is a key contributor not only to improve competitiveness in nuclear power plants, but to reduce the implementation costs of digital systems as well. The numbers of an I&C systems project require effective project data management, reaching 10,000 sensors and detectors, 5,000 kilometers of cables, and a total of 1,000 tons of mass. Furthermore, the specification of I&C systems have multidisciplinary inputs and outputs. The different technical and academic backgrounds of the actors involved in the project can lead to divergences of opinion, and the decision-making process may shift to short-term solutions. Thus, increasing the risks of project delays, due to divergences between the actors involved, specification errors and delays in the implementation and validation of control hardware and software. The main objective of this study is to propose a methodology to clarify the main data flows in an enterprise, focusing on the basic design of I&C systems. The proposed method aims to manage and apply a "top-down" specification structuring, focusing on the definition of control functions, requirements, I&C architectures, interface management, and which, in addition, ensures the application of the constructal law in the specification of these systems. The result of the methodology is to ensure that all actors involved have a global view of the entire functional analysis and definition of requirements from the highest level (UNM level) to the lower levels (of equipment specification), ensuring the passage of flows information, ensuring security, reducing project deadlines and costs.

Keywords: I&C – Instrumentation and Control Systems; Nuclear Power Plant Architecture; Guide for evaluation of Functional and Requirement analysis; SMR – Small Modular Reactor; Mobile Nuclear Power Plant

LISTA DE TABELAS E GRÁFICOS

Páginas

Tabela 1 - Exemplos de normas que se referem a sistemas I&C 38

Tabela 2 - Hipóteses para atendimento à Lei Construtal 42

Tabela 3 - Atividades vs. Hipóteses da Lei Construtal 46

Tabela 4 - Correlação entre as diversas classificações de segurança 56

Tabela 5 - Conceituação das linhas de defesa pela U.S. EPR 64

Tabela 6 - Respostas da linha metodológica à aplicabilidade da lei construtal 81

Tabela 7 - Requisitos da lei construtal na metodologia do trabalho 82

Tabela 8 - Terminologia de I&C 93

Tabela 9 - Matriz de atendimento aos requisitos à Luz da Lei Construtal 97

Tabela 10 – Exemplo de especificação do escopo funcional 109

Tabela 11 – Exemplo de especificação dos meios de Operação 111

Tabela 12 - Exemplo de relatório dos meios de operação 112

Tabela 13 - Exemplo de plano tecnológico para sensores 113

Tabela 14 - Exemplo de plano tecnológico para válvulas de controle 114

Tabela 15 - Exemplo de plano tecnológico para módulos de controle 115

Tabela 16 - Exemplo declinação funcional de alto nível 117

Tabela 17 – Exemplo de declinação funcional e classificação 118

Tabela 18 – Exemplo de tabela base com categorias funcionais 120

Tabela 19 – Exemplo de Relatório dos Blocos de Função 120

Tabela 20 - Exemplo de especificação de interfaces funcionais e condições da UNM 122

Tabela 21 - Exemplo de resultado das interfaces 122

Tabela 22 - Exemplo de especificação de malhas de controle (necessidades) 124

Tabela 23 - Exemplo de especificação de malhas de controle (Meios) 125

Tabela 24 - Exemplo de especificação de interfaces típicas para sensores 128

Tabela 25 - Exemplo de especificação de interfaces típicas para atuadores 130

Tabela 26 - Exemplo de especificação de declinação de funções ativas 131

Tabela 27 - Exemplo de alocação das malhas de controle 132

Tabela 28 - Exemplo de relatórios ES e FC..... 133

Tabela 29 - Exemplo de especificação - Declinação sistêmica 134

Tabela 30 - Exemplo de especificação - Funções de Serviço..... 134

Tabela 31 - Exemplo de especificação - Interfaces 135

Tabela 32 - Exemplo de especificação - Arranjo dos equipamentos..... 137

Tabela 33 - Exemplo de especificação - Lista de equipamentos 138

Tabela 34 - Exemplo de especificação - Requisitos funcionais..... 139

Tabela 35 - Exemplo de especificação - Requisitos dos equipamentos 139

Tabela 36 - Exemplo de especificação - Balanço de peso..... 140

Tabela 37 - Exemplo de especificação - Balanço elétrico e térmico 141

Tabela 38 - Exemplo de especificação - Requisitos de SNN 141

Tabela 39 - Exemplo de especificação - Requisitos de SNU 142

Tabela 40 - Exemplo de especificação - Requisitos de PRO..... 142

Tabela 41 - Exemplo de especificação - Requisitos de CML..... 142

Tabela 42 - Exemplo de especificação - Requisitos de STQ..... 143

Tabela 43 - Exemplo de especificação - Função e estados da UNM..... 144

Tabela 44 - Exemplo de especificação - Descrição das fases..... 145

LISTA DE ILUSTRAÇÕES

Páginas

Figura 1 - Visão geral das fases de um ciclo de vida de um projeto 19

Figura 2 - Multidisciplinariedade dos sistemas de I&C 21

Figura 3 - Visão geral das funções de controle de uma UNM..... 25

Figura 4 - Pirâmide de Automação 26

Figura 5 - Conceito básico de sistema 28

Figura 6 - Ciclo de Vida em V de Sistemas de I&C..... 30

Figura 7 - Categorias de requisitos que impactam projetos de Sistemas de I&C 33

Figura 8 - Modelo espiral de processo de projetos 34

Figura 9 - Ciclo de Vida em V simplificado e respectivas fases 48

Figura 10 - Macrovisão da fase do projeto básico 49

Figura 11 - Macrovisão das interfaces entre o projeto e a obtenção..... 49

Figura 12 - Macrovisão da base metodológica para segurança nuclear 50

Figura 13 - Estratégia “de cima para baixo” dos princípios de segurança nuclear..... 51

Figura 14 - Níveis de DiD, Barreiras de Proteção e Estados da UNM..... 54

Figura 15 - Visão geral da classificação funcional de segurança nuclear 57

Figura 16 - Macrovisão do escopo funcional..... 58

Figura 17 - Alocação funcional na Arquitetura DiD 65

Figura 18 - Distribuição dos requisitos de projeto à luz da Lei Construtal 83

Figura 19 - Estratificação dos requisitos por atividade da metodologia..... 84

Figura 20 - Correlação - CSN e condições da planta..... 107

Figura 21 - Correlação - condições da planta e dose limite (ANSI/ANS 51.1)..... 108

Figura 22 - Exemplo de especificação de arquitetura global e interfaces 123

Figura 23 - Exemplo de especificação de arquiteturas típicas para sensores 127

Figura 24 - Exemplo de especificação de arquiteturas típicas para atuadores..... 129

Figura 25 - Exemplo de especificação - Arquitetura física básica 136

Figura 26 - Exemplo de especificação – Arranjo geral da UNM 137

Figura 27 - Diagrama de estados 144

LISTA DE ABREVIATURAS E/OU SIGLAS

A – Non-safety-related with augmented requirements
AGUNM – Arquiteto Geral da Unidade Nuclear Móvel
ALARA – As low as reasonably achievable
ALARP – As low as reasonably practicable
ANSI – American National Standards Institute
AOO – Anticipated operational occurrences
ATWS – Anticipated Transient Without Scram
BTP – Branch Technical Position
CCF – Common Cause Failure (Falha de Causa Comum)
CFR – Code of Federal Regulations
CMF – Common Mode Failure (Falha de Modo Comum)
CML – Construtibilidade, Mantenibilidade e Logística
CMMI – Capability Maturity Model Integration
CNEN – Comissão Nacional de Energia Nuclear
CNRA – Committee on Nuclear Regulatory Activities (OECD-NEA)
D3 – Defense-in-Depth and Diversity
DAS – Diverse actuation system
DBA – Design basis accidents
DBE – Design basis event
DEC – Design extension criteria
DICTF – Digital Instrumentation & Control Task Force
DICWG – Digital Instrumentation and Control Working Group
DiD – Defence in depth
ECUNM – Equipe de Controle da Unidade Nuclear Móvel
EI – Eventos Iniciadores
EIA – Electronic Industries Alliance
EPRI - Electric Power Research Institute
EPUNM – Equipe de Processo da Unidade Nuclear Móvel
ES – Entrada e Saída de Dados de Instrumentação e Controle
ESF – Engineered Safety Features
FC – Funções de Controle

FIS – Função Importante para a Segurança Nuclear

FSE – Functions, systems and equipment

GDC – General Design Criteria

HFE – Human factors engineering

HMI – Human machine interface

HVAC – Heating ventilation and air conditioning

I&C – Instrumentação e Controle - Instrumentation and control

I/O ou IO – Input and Output of Data

IAEA – International Atomic Energy Agency

IEC – International Electrotechnical Commission

IEC – International Electrotechnical Commission

IEEE – Institute of Electrical and Electronics Engineers

INIS – International Nuclear Information System

INSAG - International Nuclear Safety Group

IPEN – Instituto de Pesquisas Energéticas e Nucleares

ISO – International Organization for Standardization

LOCA – Loss of Coolant Accident

LWR – Nuclear Power Plants

MLA – Modern Language Association

N – Non-safety-related

NBR – Norma Brasileira

NRC – Nuclear Regulatory Commission

NSC – Nuclear Safety Classification

NUREG – Nuclear Regulatory publications

OpC – Operation concepts

PIE – Postulated initiating event

PMBOK – Project Management Body of Knowledge

PMI – Project Management Institute

PRA - Probabilistic Risk Assessment

PRO – Projeto

Q – Safety-related

RCPB – Reactor Coolant Pressure Boundary

RT – Reactor Trip

SBO – Station Blackout

SCRAM – Sudden shutting down of a nuclear reactor

SDO – Standards development organization

SE – System Engineering

SIS – Sistema Instrumentado de Segurança

SNN – Segurança Não Nuclear

SNU – Segurança Nuclear

SSC – Structures, systems and components

STQ – Segurança do Trabalho e Qualidade

STUK – Radiation and Nuclear Safety Authority (Finland)

U.S. NRC – United States Nuclear Regulatory Commission

UNM – Unidade Nuclear Móvel

USP – Universidade de São Paulo

WENRA – Western European Nuclear Regulators Association

WG – Working group

WGDIC – Working Group Digital I&C (OECD-NEA CNRA)

WNA – World Nuclear Association

YVL – Regulatory guides on nuclear safety (Finland)

SUMÁRIO

Páginas

1 INTRODUÇÃO 17
1.1 Objetivos 21
1.1.1 Objetivo geral 21
1.1.2 Objetivos específicos 21
1.2 Justificativa 22
2 REVISÃO DA LITERATURA 24
2.1 A importância dos Sistemas de Instrumentação e Controle: breve contexto 24
2.2 Sistemas I&C e a engenharia de sistemas 26
2.3 Sistemas I&C e o Ciclo de Vida ("*Life Cycle*") 29
2.4 Sistemas de I&C e a Base de Projeto ("*Design Basis*") 31
2.5 Sistemas I&C e a importância para a segurança nuclear 35
2.6 Sistemas I&C e as principais bases normativas 36
3 METODOLOGIA 41
3.1 Tipo de estudo 41
3.2 Delineamento da pesquisa 41
3.3 Embasamento teórico 43
3.4 Desenvolvimento da metodologia 46
3.4.1 Levantamento de requisitos metodológicos para a especificação de sistemas de I&C de usina nuclear móvel 46
3.4.2 Proposição da linha metodologia 47
3.4.3 Proposição de implementação da linha metodológica 51
3.4.4 Critérios gerais de I&C (Especificação de requisitos transversos) 52
3.4.4.1 Delimitação do escopo dos Sistemas de I&C 53
3.4.4.2 Especificação dos meios disponíveis de operação 59
3.4.4.3 Plano Tecnológico de I&C 62
3.4.5 Arquiteturas funcionais de I&C (Especificação de interfaces transversas) 63
3.4.5.1 Declinação funcional e classificação dos sistemas de I&C 66

3.4.5.2 Interfaces Funcionais e Condições da Planta 68
3.4.5.3 Arquitetura funcional – Global de I&C 69
3.4.6 Arquiteturas típicas de I&C (Especificação dos dados de entrada): 69
3.4.6.1 Especificação das malhas de I&C 70
3.4.6.2 Catalogação das arquiteturas típicas 71
3.4.6.3 Alocação das malhas de I&C 73
3.4.6.4 Geração de relatórios de Entrada e Saída e de funções de controle. 73
3.4.7 Especificação de sistemas de controle 74
3.4.7.1 Descrição do Sistema de Controle 75
3.4.7.2 Caracterização do Sistema de Controle 76
3.4.7.3 Operação do Sistema de Controle 78
4 RESULTADOS E DISCUSSÃO 80
4.1 Atendimentos aos requisitos da Lei Construtal 80
4.2 Análise e discussão dos dados 82
5 CONCLUSÃO 85
6 CONTRIBUIÇÕES DESTE ESTUDO 87
REFERÊNCIAS BIBLIOGRÁFICAS 88
ANEXO 1 – Terminologias e conceitos relativos à engenharia de sistema 93
ANEXO 2 – Lista de requisitos e suas justificativas 97
ANEXO 3 – Correlação de classificações e condições da planta 107
ANEXO 4 – Modelos para as especificações dos Sistemas de I&C 109

1 INTRODUÇÃO

Atualmente o transporte marítimo é responsável por 95% do comércio mundial e tem papel central na economia e prosperidade dos povos (ROYAL ACADEMY OF ENGINEERING, 2013). Levando-se em consideração que o preço de combustíveis nucleares tem volatilidade inferior ao do petróleo, pois o fornecimento de urânio se dá por meio de contratos de longo prazo diferentemente do petróleo cujo preço é negociado diariamente (FREIRE e DE ANDRADE, 2017; MARI, 2014; MCMAHON, 2017), não é de se estranhar que a partir do final da década de 50 já se apresentassem embarcações mercantes que utilizassem a sua propulsão com origem nuclear, como por exemplo, os navios mercantes norte-americanos NS SAVANNAH (LANGE, 1990) (OFFICE OF SHIP DISPOSAL - MARITIME ADMINISTRATION, 2011), alemão OTTO HAHN (CINTRA, 2016), japonês MUTSU (NAKAO, 1992) e russo SERVMORPUT (FREIRE, 2018).

Para as grandes potências a opção nuclear pode se tornar uma tecnologia competitiva (O'ROURKE, 2010), pois embora a opção por propulsão nuclear tenha um custo superior de aquisição, estas apresentam custos de combustíveis inferiores aos de navios movidos a combustíveis fósseis (FREIRE e DE ANDRADE, 2017). Outro fator que também pode ser levado em consideração é que essas usinas não produzem gases que contribuem para o efeito estufa, ao contrário dos navios movidos a combustível fóssil.

Sendo assim, se faz necessário procurar métodos para redução do custo de aquisição de uma Usina Nuclear Móvel (UNM) mantendo os riscos à segurança dentro dos limites aceitáveis. Para isso organismos internacionais, governos e empresas tem procurado implantar metodologias e ferramentas para gestão de projetos.

Face ao exposto, este trabalho visa propor uma metodologia de especificação de sistemas de instrumentação e controle (I&C) levando-se em consideração o trabalho desenvolvido por FREIRE (2018), tendo em vista que a literatura acadêmica não dispõe de uma ampla pesquisa sobre os métodos para especificação de sistemas de I&C de UNMs baseados na facilitação do fluxo de informações num projeto.

Além disso, o trabalho se torna relevante devido à complexidade e transversalidade que envolve os sistemas de I&C dentro de um empreendimento nuclear. Estudos apontam que inicialmente os custos envolvidos para o projeto e ciclo de vida de um sistema I&C são preteridos em relação a outros grandes sistemas e equipamentos

nucleares, contudo seu impacto para a disponibilidade, segurança e desempenho da planta são substanciais (HURST, 2007).

Como bem alerta HASHEMIAN (2011), assumindo que uma UNM de 1000 MW elétricos traz uma receita bruta de cerca de U$ 2 milhões por dia, a perda de níveis de produção de potência de até um por cento pode gerar milhões de dólares de prejuízo.

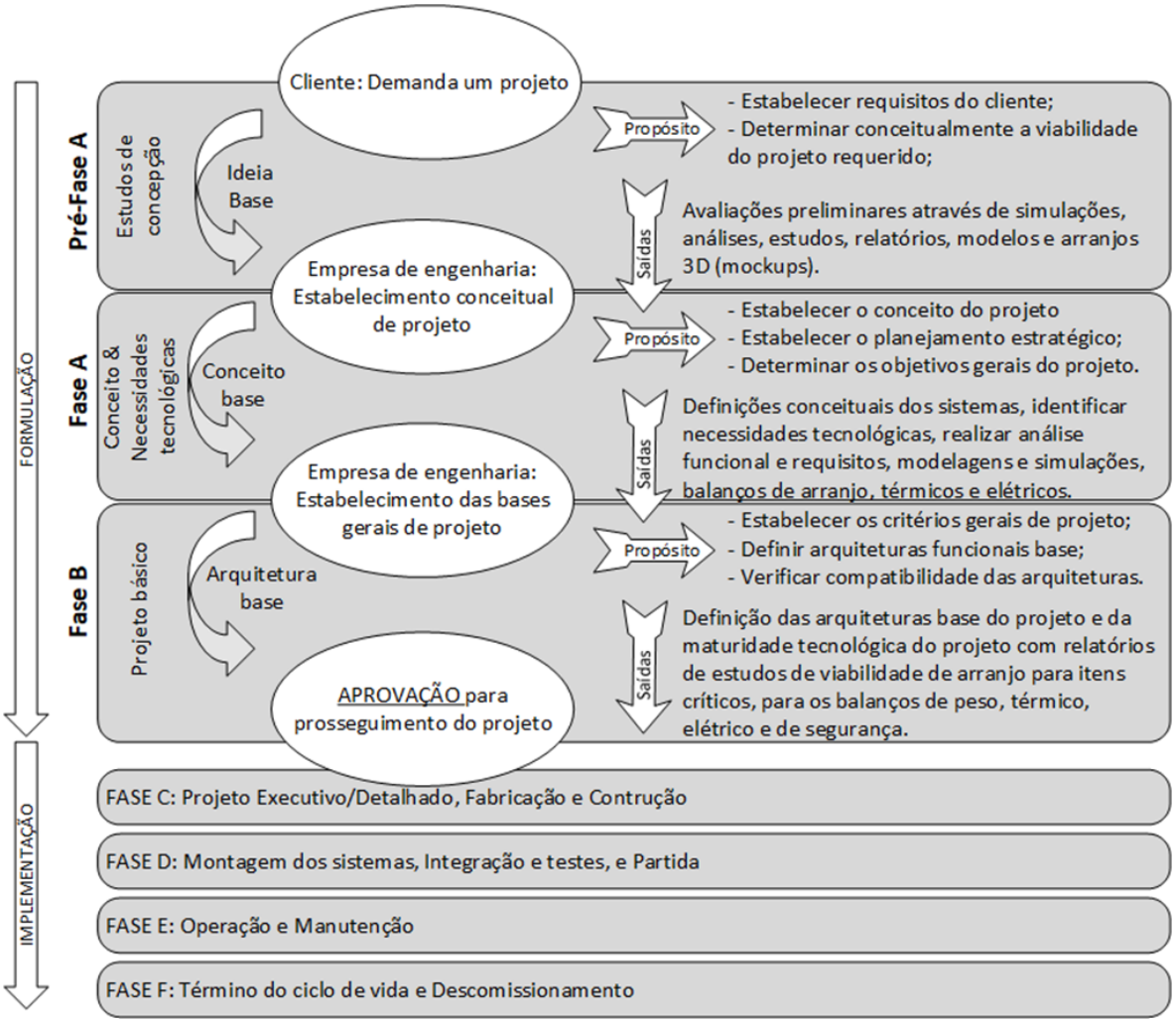
Além disso, erros de especificação devido à complexidade de sistemas I&C, podem gerar retrabalhos no projeto executivo, construção, integração, validação, partida, operação e manutenção da planta, até mesmo no seu descomissionamento. Numa planta nuclear, a instrumentação possui tipicamente 10.000 sensores e detectores, podendo chegar a cerca de 5.000 quilômetros de cabos que representam a ordem de 1.000 toneladas de massa (HASHEMIAN, 2011), ou seja, ordens de peso e volume que poderiam inviabilizar a implantação de UNMs.

Parte da causa deste problema (retrabalhos e atrasos) está na estruturação e definição de atribuições dentro das equipes de projeto, visto que a especificação de sistemas de I&C tem entradas e saídas multidisciplinares. As diferentes formações técnicas e acadêmicas podem conduzir a divergências de opinião, e o processo decisório grande parte das vezes inclinam-se para as soluções de curto prazo, gerando riscos futuros no que se referem aos testes de integração, desempenho, partida e início de operação da UNM, como já citado anteriormente.

Este risco deve ser considerado pelas equipes de planejamento, para que as atividades previstas no cronograma não acarretem consequências diversas no futuro. Tipicamente, o início de uma fase de projeto detalhado requer o amadurecimento do projeto básico, em níveis de riscos aceitáveis, que não inviabilizem a conclusão do empreendimento. Por isso, sobre o projeto básico recaem pontos graves de especificação. No caso de sistemas de I&C, discordâncias entre as equipes de processo e controle são recorrentes, devido à simbiose existente entre elas.

Na figura 1 é explicitado simplificadamente todo o ciclo de projeto, tomando como base o conceito da NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (2007), que divide o projeto em sete fases, agrupadas em duas grandes categorias: formulação e implementação. Note que a implementação do projeto requer uma aprovação de alto nível (entre cliente e projetista), ratificando que o produto está maduro tecnologicamente, aderente aos requisitos e critérios definidos em alto nível.

Figura 1 - Visão geral das fases de um ciclo de vida de um projeto



Fonte: adaptado de NASA, 2007.

As Equipes de Processo da UNM (EPUNM) são tipicamente formadas por engenheiros químicos, a quem cabe a especificação funcional e dos critérios que definirão a arquitetura dos sistemas que processam as grandezas físico-químicas. Para isso, se faz mister especificar meios de se monitorar e manipular as variáveis de processo, através de sensores, bombas, válvulas, aquecedores, tanques, vasos de pressão, etc.

As Equipes de Controle da UNM (ECUNM) são tipicamente formadas por grupos interdisciplinares que abarcam desde eletroeletrônicos e de computação, a quem cabe a especificação funcional e dos critérios que definirão a arquitetura dos sistemas que controlam aqueles sistemas que processam as grandezas físico-químicas. Para isso, se faz mister especificar meios de se controlar as variáveis de processo, através de controladores e estações de supervisão para os operadores da UNM.

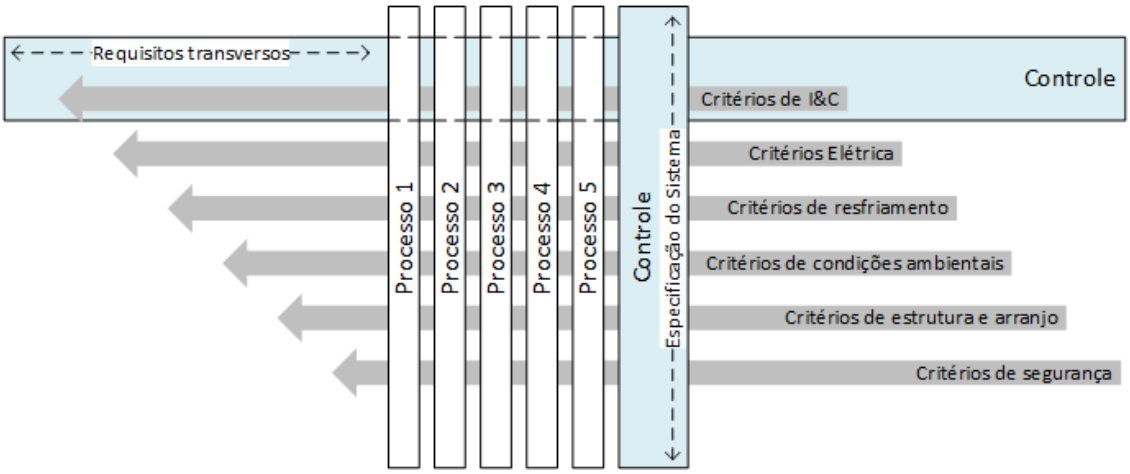
Notemos assim, a linha tênue que divide as duas equipes na responsabilidade de especificação de sistemas de I&C, principalmente numa fase tão importante como é o projeto básico. Resumidamente, podemos afirmar que a ECUNM é servidora da EPUNM, ou seja, cabe ao processo definir o que o controle deve implementar. Isto é algo aparentemente óbvio de se notar, entretanto no andamento do projeto podem ocorrer conflitos na definição de escopo. A EPUNM pode, por exemplo, associar que cabe à ECUNM a responsabilidade de definir a operação dos sistemas de processo. Da mesma forma, pode a ECUNM pensar que a definição da operação só cabe ao dono dos sistemas, as EPUNM.

Isto pode ser muito danoso para o andamento do projeto, pois caso não haja um planejamento em alto nível que defina claramente estes escopos, os conflitos de atribuições podem gerar ruídos entre os atores envolvidos. Além disso, a ECUNM pode inclusive pensar que o início dos seus trabalhos ocorre apenas após as especificações das EPUNM, aumentando o risco de atrasos nas atividades.

Daí decorrem alguns questionamentos fundamentais para o planejamento das atividades das ECUNM, e que nem sempre são claras. Então, o que pode ser feito sem dados ou especificações das EPUNM? Como saber se os dados das EPUNM estão maduros o suficiente para serem considerados? Depois, como saber se as especificações (que vão para o fabricante do sistema de controle) atendem às especificações do EPUNM? E depois, como saber se o que o fabricante fez está atendendo às especificações da ECUNM? E depois, como fazer correções, evoluções e melhorias sem desfazer o que foi feito?

Desta forma, é urgente que no projeto básico estejam sanadas todas estas questões, e para isso é preciso entender a natureza dos sistemas de I&C dentro de um projeto. Os sistemas de I&C tem a característica de serem ao mesmo tempo horizontais e verticais na sua concepção, implementação e integração, como pode ser verificado na figura 2. Verticais naquilo que se refere às especificações técnicas da sua arquitetura de controle (parte dos sistemas de I&C), e no que envolve trâmites documentais com fabricantes. Horizontais naquilo que se refere aos critérios gerais a serem atendidos pelas outras disciplinas de processo a serem controladas, tanto pelos conceitos de operação definidos em alto nível em conjunto com o arquiteto geral do projeto (AGUNM), pelos meios a serem disponibilizados para controle e monitoramento da UNM, e pelos critérios a serem atendidos nos níveis mais inferiores (sensores, atuadores e controladores locais – parte dos sistemas de I&C).

Figura 2 - Multidisciplinariedade dos sistemas de I&C



Deve-se salientar que a transversalidade dos Sistemas de I&C requerem trocas de informações e gerações de interfaces de projeto que não são evidenciadas fisicamente com clareza. Isto requer um entendimento global, de que uma interface física de dados pode atender a diversas necessidades funcionais. Portanto, a transversalidade requer que a ECUNM disponibilize os critérios de projeto necessários, e que as EPUNM requeiram do controle o serviço necessário através de especificações de operação.

1.1 Objetivos

1.1.1 Objetivo geral

Elaboração de uma metodologia de especificação de sistemas de Instrumentação e Controle (I&C) para usinas nucleares móveis, em nível de projeto básico, levando-se em consideração a tese desenvolvida por FREIRE (2018): de facilitação do fluxo de informações visando todo o ciclo de vida de um empreendimento, orientado pelos princípios da lei construtal. Definir, portanto, o conjunto mínimo de especificações das funções de controle e interfaces (requisitos funcionais) e de especificações do hardware (requisitos não funcionais).

1.1.2 Objetivos específicos

Definir modelos (*templates*) para os documentos de projeto básico de sistemas de I&C, e justificar os elementos dos modelos em que haja:

a) Estabelecimento claro das bases de projeto para viabilizar a especificação de sistemas de I&C.
b) Estabelecimento de formato específico de análise funcional com respectivas classificações segundo os objetivos gerais de segurança nuclear e de uma planta nuclear móvel (de disponibilidade e segurança).
c) Estabelecimento de uma arquitetura geral de I&C com base nas camadas de automação industrial (sensores e atuadores, dispositivos controladores de campo, sistemas de controle de processo, sistema de supervisório e de informações, e sistema de gerenciamento de informações técnicas), e na filosofia de defesa em profundidade e diversidade (DiD ou D3) previstos no projeto;
d) Alocação das funções de controle (de serviço e/ou técnicas) a serem executadas em cada sistema de I&C. Estas funções de controle são definidas pelas instalações a serem controladas, e as demandas devem ser claramente identificadas no projeto, para facilitação do fluxo de informações entre os atores envolvidos - Sistemas, Estruturas, Componentes (SSCs);
e) Alocação das funções de cada sistema de I&C e respectivas interfaces funcionais, que definirão as interfaces de dados (protocolo e fluxo de sinal) entre os diversos sistemas da UNM.
f) Elaboração e catalogação de arquiteturas típicas de controle para atendimento à UNM como um todo, buscando-se assim a padronização da filosofia de I&C para o monitoramento e controle das SCCs;
g) Catalogação das malhas de I&C, classificação conforme as funções de controle estabelecidas, alocação nos níveis de DiD ou D3 previstos, e direcionamento à arquitetura típica específica, para geração de relatórios de entrada e saída de dados (I/O).

1.2 Justificativa

Seguindo a preocupação apontada por FREIRE et al. (2018) de que a literatura hoje ainda não dispõe de publicações que englobem o conhecimento comportamental de um sistema com profundidade (embora seja desejável em qualquer projeto), faz-se mister

o estudo de metodologias de especificação de projeto que olhem com cuidado o comportamento dos diversos sistemas de uma UNM em conjunto com os sistemas de I&C, tendo-se em vista a lei construtal.

Os relacionamentos entre tempo, crédito, informação e realização são fontes de atenção constantes dentro de uma organização (FREIRE; DE ANDRADE; 2018). A facilitação do fluxo de informações em projetos de I&C converge para a amenização dessa preocupação nos grandes empreendimentos. Ferramentas de extração de dados sob demanda e maduros o suficiente para estimativas de custo, homem-hora, e pré-especificação de equipamentos de sistemas I&C, são objetos de interesse de estudos.

Diante disso, há uma lacuna na literatura com proposições de metodologias e ferramentas de especificação dedicada aos sistemas I&C que sigam os conceitos de análise funcional (CHERNYAEV et al., 2017), apliquem a conceituação de banco de dados relacional ou ferramenta baseada em modelos, e permitam a consistência de informações dentro de padrões de qualidade aceitáveis.

Ferramentas deste tipo, baseada em metodologias fundamentadas na lei construtal, facilitariam e agilizariam a verificação e validação do projeto (soluções técnicas e/ou produtos) frente às especificações definidas em todo ciclo de vida de sistemas I&C.

2 REVISÃO DA LITERATURA

2.1 A importância dos Sistemas de Instrumentação e Controle: breve contexto

Os sistemas de I&C são fundamentais dentro de qualquer instalação. Do mesmo modo, não há como conceber uma planta nuclear sem sistemas de I&C confiáveis que forneçam as informações necessárias para se garantir a operabilidade dentro dos parâmetros de disponibilidade e segurança para qual foi projetada.

Estes sistemas são responsáveis por prover todos os controles manuais, semiautomáticos ou automáticos durante operação normal, condições anormais antecipatórias (AOO) e acidentais. Estes controles podem ser intertravamentos ou de regulagem contínua, e ainda permitir monitoramento geral da planta pelo operador de forma que seja possível executar ações corretivas ou preventivas para a manutenção da planta em condições seguras, e disponível ao seu propósito de gerar energia.

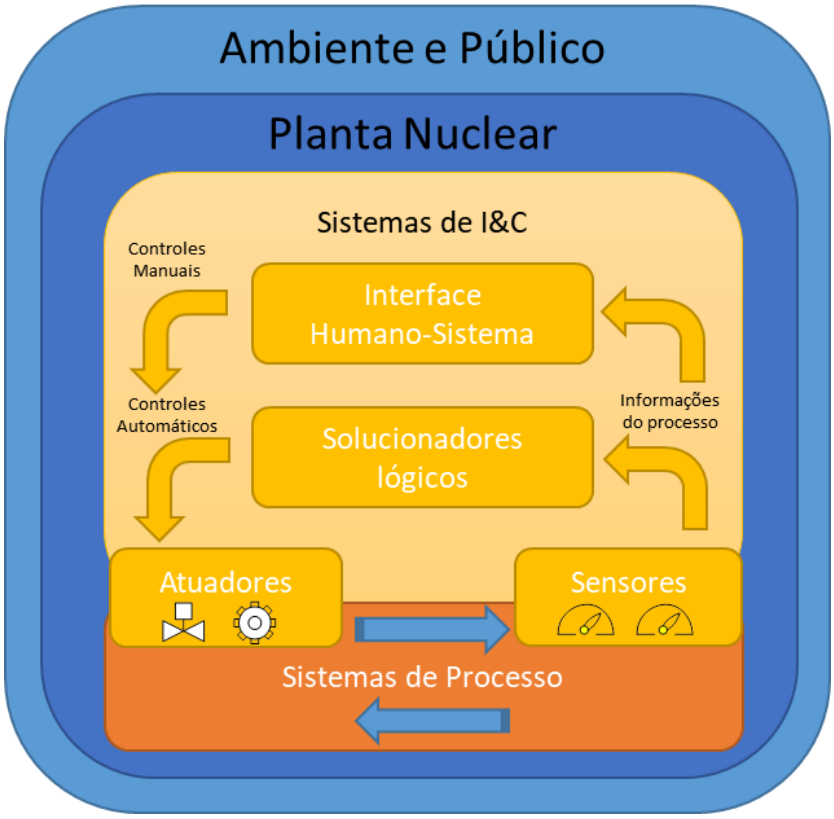
Para prover tais funções, os sistemas de I&C são compostos basicamente por sensores (para realizar a medição dos parâmetros do processo – variável medida), os controladores (para realizar a lógica de controle) e os elementos finais de controle (para executar ou atuar em algum parâmetro da planta – variável manipulada). Obviamente, os sistemas I&C abarcam também outros componentes que são interfaces com o operador da planta (HSI – "*Human-System Interface*", HMI – "*Humam-Machine Interface*", etc.), ou ainda sistemas computadorizados com seus sistemas de comunicação associados (tais como as redes de computadores) ou softwares, e ainda dispositivos que são programados usando linguagens de hardware (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016).

Garantir a devida especificação é fator preponderante para que os sistemas de I&C sejam capazes de proteger a planta contra erros humanos (operacionais ou não), ou ainda falhas aleatórias de alguma SSC. Para isso os sistemas de I&C devem ser capazes de executar ações automáticas com rapidez. O objetivo vai além do propósito de se produzir energia, isto é, garantir a integridade da planta e proteger os trabalhadores e o meio ambiente de vazamentos radiativos certamente é o objetivo mais restritivo para se alcançar.

Portanto, para garantir que os parâmetros da planta estejam dentro dos limites de projeto, a informação deve ter a acurácia e confiabilidade necessárias. Estas informações são providas por sensores (temperatura, umidade, pressão, nível, vazão, posição etc.). Posteriormente, os valores destas medidas são comparados com os valores de "*set-point*" previamente estabelecidos nos controladores ou procedimentos. Dependendo do desvio identificado, ações corretivas serão executadas pelos atuadores, a partir de um controle automático ou manual.

Cabe mencionar também, que para melhor hierarquização das funções de controle apresentadas na figura 3, utiliza-se uma estruturação de comunicação nas arquiteturas de sistemas de I&C.

Figura 3 - Visão geral das funções de controle de uma UNM

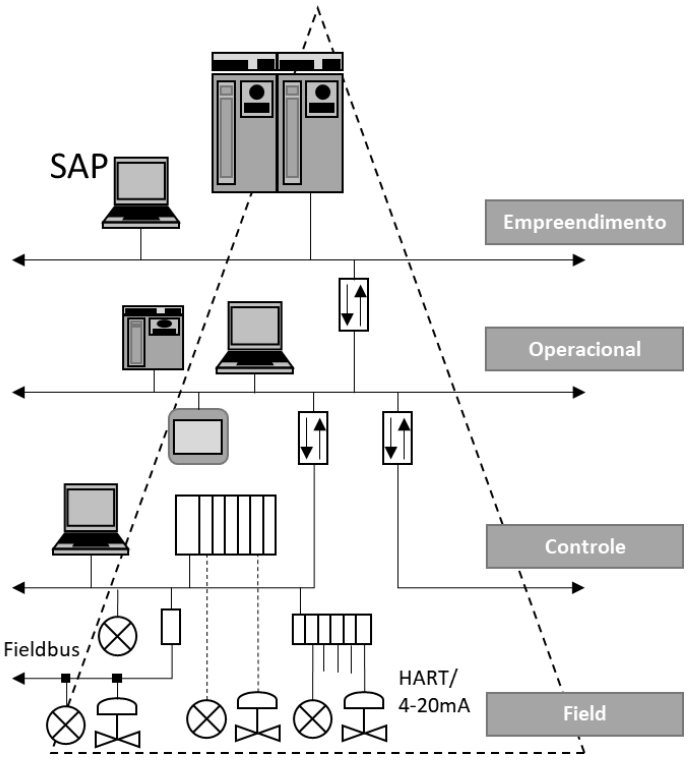


Fonte: adaptado de IAEA, 2011.

A estrutura é remontada na figura 4, num modelo também conhecido como "Pirâmide de Automação Industrial". Esta pirâmide elenca os níveis de automação necessários: nível de campo ou processo (que compreende os sensores e atuadores), nível

de controle (onde se processa os sinais de monitoramento e comando dos elementos do processo), nível de operação (que compreende os meios de intervenção e monitoramento do processo pelo operador), e por fim o nível de empreendimento (que compreende os dados reportados para a gerência operativa, administrativa e planejamento). (LIPTÁK, 2006).

Figura 4 - Pirâmide de Automação



Fonte: adaptado de LIPTAK, 2006.

2.2 Sistemas I&C e a engenharia de sistemas

A partir desta demarcação genérica do que seriam os sistemas de I&C, é necessário harmonizar o entendimento conceitual básico sobre engenharia de sistemas. Não é escopo deste trabalho se aprofundar na teoria de sistemas, contudo é urgente estabelecer bases conceituais e premissas para que a metodologia não se perca naqueles conceitos mais fundamentais, e na clara definição do escopo dos atores envolvidos.

Explorando a literatura acerca do assunto, decidiu-se atender plenamente a conceituação da NASA, também utilizada na tese de FREIRE (2018), em que:

> *A engenharia de sistemas é um campo interdisciplinar da engenharia com foco na maneira de gerenciar e projetar sistemas complexos ao longo de todo o seu ciclo de vida.* (FREIRE, 2018, P.27).

A literatura dispõe de uma infinidade de teorias acerca do assunto ALVES (2012), BERTALANFFY (2008) e HALL (1962) para garantir a convergência aos princípios da lei construtal e das hipóteses por FREIRE (2018) levantadas. Sistemas complexos por definição é um conjunto sistêmico que abarca relacionamentos de diferentes entes com vistas à gerenciar a troca de informações e serviços entre o processo (ideias e regras), o capital-humano (pessoas) e as ferramentas (recursos, matéria-prima e equipamentos) (FREIRE, 2018).

A lei construtal é um princípio que garante a evolução permanente da facilitação de fluxos (termodinâmicos, energia, entidades mentais etc.) para sua sobrevivência e permanência ao longo do tempo. A lei construtal é portanto um princípio que garante a economia de escala em todas as fases do ciclo de vida de sistemas complexos, pois estes demandam maior facilitação de fluxo frente ao desafio de se reduzir riscos associados ao ciclo de vida (FREIRE, 2018).

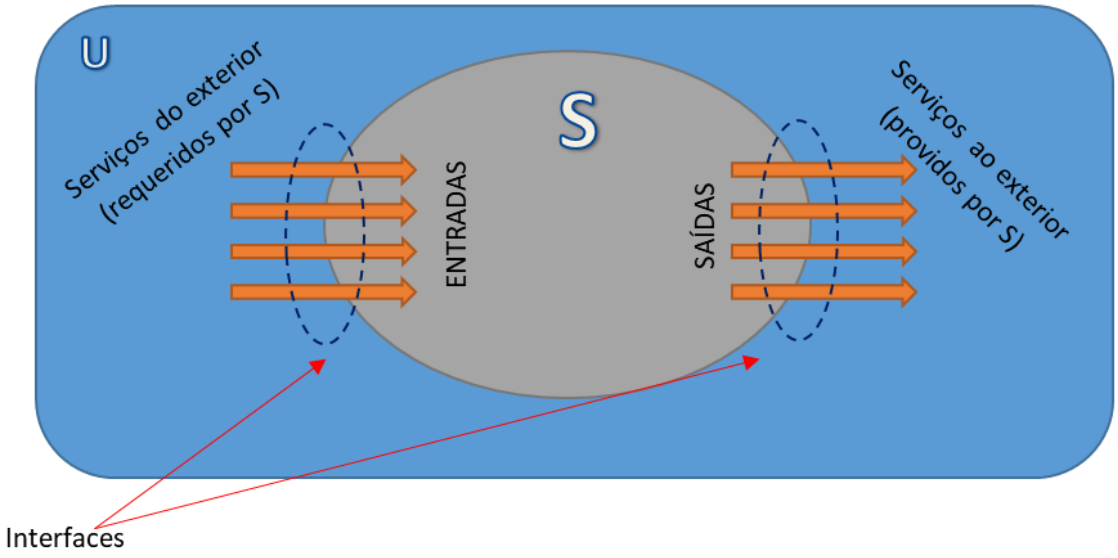
Há um favorecimento em âmbito mundial ao aumento de sistemas complexos. Estes sistemas não podem ser especificados por um único homem ou equipe limitada, principalmente se o empreendimento foi concebido baseado em documentação ("*document based*"). Logo, urge a necessidade de ferramentas baseadas em modelos ("*model based*") de ciclos de vida que visem garantir o atendimento dos princípios da lei construtal em todo o ciclo de vida de um sistema (FREIRE, 2018).

Todavia, a primeira pergunta que se faz é: o que é um sistema? Seguindo a abordagem normativa da INTERNATIONAL ORGANIZATION FOR STANDARDIZATION e THE INTERNATIONAL ELECTROTECHNICAL COMMISSION (2015), podemos afirmar que um sistema é uma combinação de interações dos elementos do sistema, organizados para atingir um ou mais estados propostos. E quem seriam estes elementos do sistema? A mesma norma delineia que tais elementos seriam dispositivos, estruturas, software, dados, humanos, procedimentos, materiais, ou qualquer entidade da natureza (água, vapor, ar, minerais etc.).

Neste sentido, conforme se apresentado na figura 5, sistema é um conjunto S dentro de um universo de elementos U, ou seja, U contêm S. Os elementos de S realizam funções para o exterior do conjunto S, e S recebe funções de outros elementos pertencentes a U e que não pertencem a S. Estas interações entre o universo no interior e exterior de S são chamadas de interfaces funcionais, ou seja, são superfícies de contato entre os diversos sistemas e onde ocorrem as transferências de massa, energia, informação, em suma, onde há os fluxos de que trata a lei construtal (FREIRE, 2018).

Em toda interface há um ator responsável (quem demanda) e um coadjuvante (quem fornece) FREIRE (2018). E talvez ai esteja o elo mais frágil de todo projeto. A interface é onde ocorre a interação entre os diversos atores. A determinação de quem é o responsável por tal interface deve ser clara e padronizada para que o princípio da lei construtal seja atendido. E esta padronização do responsável e coadjuvante de tal interface pode gerar polêmica.

Figura 5 - Conceito básico de sistema



O modo mais coerente para definição do responsável pela interface deve ser o mais simples. Por que existe tal interface? A resposta deve ser direcionada para quem ela é útil. Sendo assim, quem demanda o serviço deve ser o responsável pela interface. Questionamentos podem surgir desta premissa, pois quem desenvolverá a solução seria aquele que providencia o serviço. Contudo, quem solicita (cliente) é quem especifica o

serviço, e deve ser quem valida o serviço. Portanto o cliente é o responsável, e o provedor do serviço é o coadjuvante.

Diante deste universo sistêmico complexo, com alto número de funções, interfaces, requisitos e atores envolvidos, há de se concluir que é real a alta probabilidade de ocorrência dos riscos associados. Erros identificados nas soluções técnicas que divergem do especificado, dificuldades e mal-entendidos na comunicação entre cliente e provedor, e até desobediência consentida, são fatos que corroboram a utilização de uma metodologia (e ferramentas) que tenham como princípio as hipóteses e definições apontadas por FREIRE (2018).

2.3 Sistemas I&C e o Ciclo de Vida ("*Life Cycle*")

Sistemas de I&C são extremamente complexos, tanto pelo grande número de requisitos e interfaces, tanto pelo universo dos componentes que o compõe. Além disso, há restrições de projeto de forma geral, além dos critérios de segurança nuclear. Desta forma, para se garantir rastreabilidade, meios de qualificação e a qualidade dos requisitos, se faz mister prever um adequado ciclo de vida (STANDARDS COUNCIL OF CANADA, 2002).

O conceito de Ciclo de Vida pode ser visto como um núcleo por onde orbitam os demais campos relacionados ao projeto do sistema. Isto porque se trata de um processo de engenharia que contempla todas as fases da vida sistêmica e as respectivas necessidades. O seu propósito é garantir que nunca se perca de vista os objetivos funcionais de mais alto nível traçados desde a fase de concepção, passando pelo projeto, construção, comissionamento, partida, operação, manutenção e descomissionamento (THOMSON, 2012).

O Ciclo de Vida trata-se de um amplo planejamento. Nele contém os requisitos que visam à redução de riscos dentro de um empreendimento, riscos estes voltados principalmente para a segurança do público, trabalhadores e ambiente, além daqueles voltados para a redução dos custos de implantação e manutenção (THOMSON, 2012).

O estado da arte dos sistemas de I&C, compostos majoritariamente por sistemas digitalizados, exigem processos extensos de especificação, projeto e qualificação, além daqueles tipicamente utilizados no passado. Desta forma, surgem necessidades de um gerenciamento mais eficiente dos requisitos frente às soluções técnicas apresentadas.

Sistemas de engenharia que modelam do ciclo de vida destes sistemas são cada vez mais requeridos. A consequente utilização destes sistemas "*model based*", em lugar do "*document based*", minimizam erros e retrabalhos dentro dos projetos, e facilitam os procedimentos de manutenção e testes, e de um necessário descomissionamento.

A IAEA estabelece que num ciclo de vida de sistemas de I&C há três níveis fundamentais: Ciclo de Vida da Arquitetura Geral de I&C; Um ou mais Ciclos de Vida individuais para Sistemas de I&C; Um ou mais Ciclos de Vida individuais para componentes (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016). O framework contendo todo o Ciclo de Vida de sistema de I&C proposto pela IAEA destaca haver duas grandes interfaces, que são as interações com o programa de engenharia de fatores humanos (HFE), e com o programa de segurança cibernética.

Portanto, cabe notar que o gerenciamento de um ciclo de vida é algo extenso, com muitas fases (que podem durar anos) e consequentemente com muitos atores. Com base na lei construtal, onde a informação é um dos principais fluxos institucionais, há de se estabelecer boa qualidade nas informações utilizadas e transmitidas (reduzindo a contaminação e preservando a integridade), facilitação na troca destas informações (desburocratização: assegurando e facilitando a passagem do fluxo), e alinhamento em torno de uma cultura de segurança com programas de engenharia de fatores humanos e segurança cibernética (FREIRE, 2018).

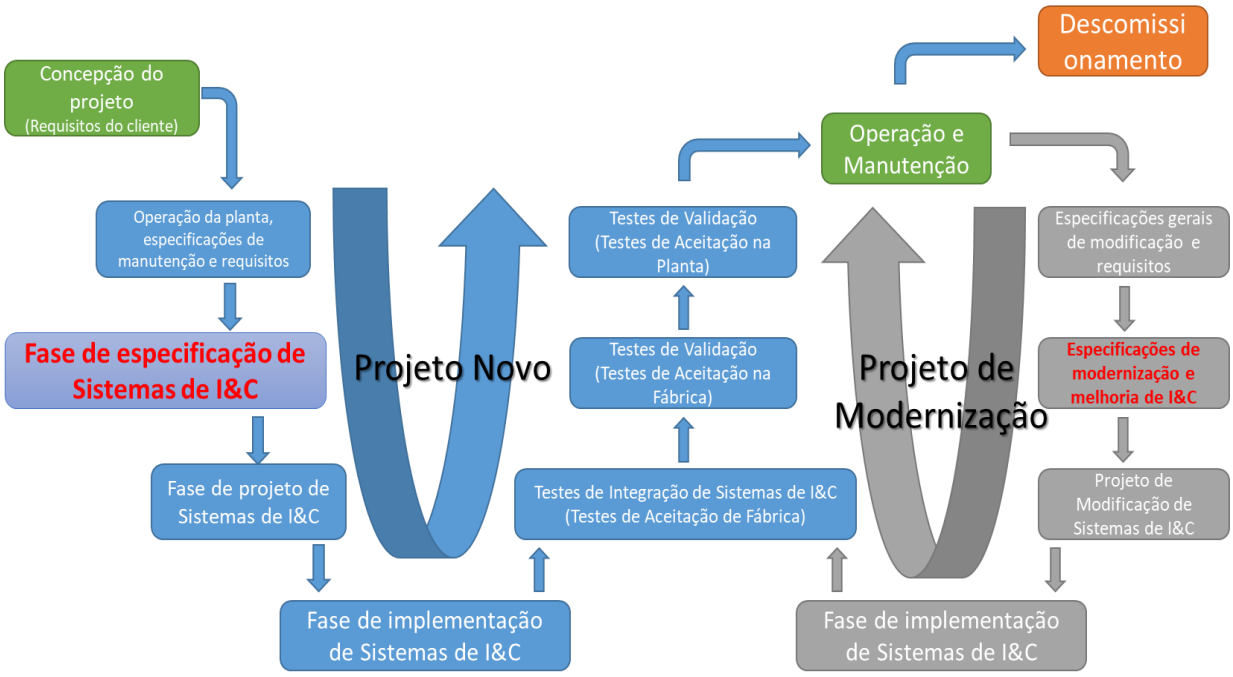
Particularmente, os órgãos reguladores estão cada vez mais exigentes para que os projetos dos sistemas digitais ou baseados em softwares contemplem especificações claras, com respectivas atividades de verificação e validação, e com os meios de demonstração, qualificação e testes para se garantir a adequabilidade de uso. Para isto, deve-se prever alta qualidade no processo de desenvolvimento, balizado por eficientes métodos de especificação e implementação dos requisitos de projeto (INTERNATIONAL ATOMIC ENERGY AGENCY, 2009).

O ciclo de vida de projeto em "Vê" apresentado na figura 6 é um método eficiente e claro de planejamento estratégico. O escopo deste trabalho está limitado a apresentar um método de especificação na decida da curva do "V-Cycle", limitando-se naquelas especificações de cima para baixo (fase de especificação de sistemas de I&C) características do projeto básico de sistemas de I&C (STANDARDS COUNCIL OF CANADA, 2002).

Esta delimitação do escopo deve-se ao fato da grande importância da fase de projeto básico. Fase esta que comporta a solidificação dos requisitos conceituais do

cliente. Boa especificação nesta fase implica em minimização dos riscos de projeto, no que se referem aos custos, prazos e segurança.

Figura 6 - Ciclo de Vida em V de Sistemas de I&C



Fonte: adaptado de IAEA, 2016.

2.4 Sistemas de I&C e a Base de Projeto ("*Design Basis*")

A especificação dos sistemas de I&C devem prever os critérios gerais definidos pelo AGUNM. O objetivo é assegurar uma operação segura, sem que se excluam considerações acerca da confiabilidade, operabilidade e manutenibilidade. Para isso, em todo o ciclo devem ser realizadas análises de segurança por uma equipe independente do projeto, para a identificação dos perigos em potencial no que se refere ao desenvolvimento do sistema de I&C, definindo, através de uma análise de risco, estratégias de redução ou até eliminação do perigo.

Isto não exclui a participação dos arquitetos dos sistemas de I&C. É fundamental que estes colaborem com o time de análise de segurança global. Contudo, a análise de segurança global da planta a ser apresentada nos relatórios de licenciamento obedece a

marcos particulares, e que nem sempre coincidem com as demandas e realidades de obtenção do projeto.

Neste sentido, é compatível que dentro do projeto haja critérios de segurança, e até análise riscos com métodos inicialmente qualitativos, ou até semiquantitativos, para que determinem mesmo que conservadoramente os objetivos das funções a serem desempenhadas pelos diversos sistemas da UNM.

Outro ponto fulcral é a definição clara da base normativa a ser utilizada no projeto, e sua formalização junto ao órgão regulador. Este marco será outro ponto de partida para se delimitar o escopo de soluções. Entretanto, um cuidado precisa ser tomado. O estabelecimento da base normativa, pode até definir como obrigatórias normas de alto nível, mas nunca as normas sucessoras para os níveis subsequentes. Tornar obrigatórios os códigos industriais, utilizados na fabricação e construção de sistemas dedicados e/ou componentes, pode inferir uma restrição demasiada, aumentando o risco de inviabilização do projeto.

Uma especificação inerentemente segura deve conter estratégias para minimizar, substituir, moderar e simplificar o projeto, e estas estratégias devem ser implementadas o quanto antes. Duas atividades críticas requeridas nesta fase, portanto são a análise funcional e especificação dos requisitos.

No que tange a análise funcional, no nível da embarcação cabe a determinação das funções de serviço a partir de uma metodologia de autonomia e disponibilidade, e a determinação das funções de segurança a partir de uma metodologia de análise de segurança em conformidade com a base normativa. Posteriormente, em nível de sistema cabe a alocação funcional (de serviço ou de segurança) a cada sistema de acordo com a estratégia adotada para a redução do risco e com a estruturação sistêmica adotada pela planta.

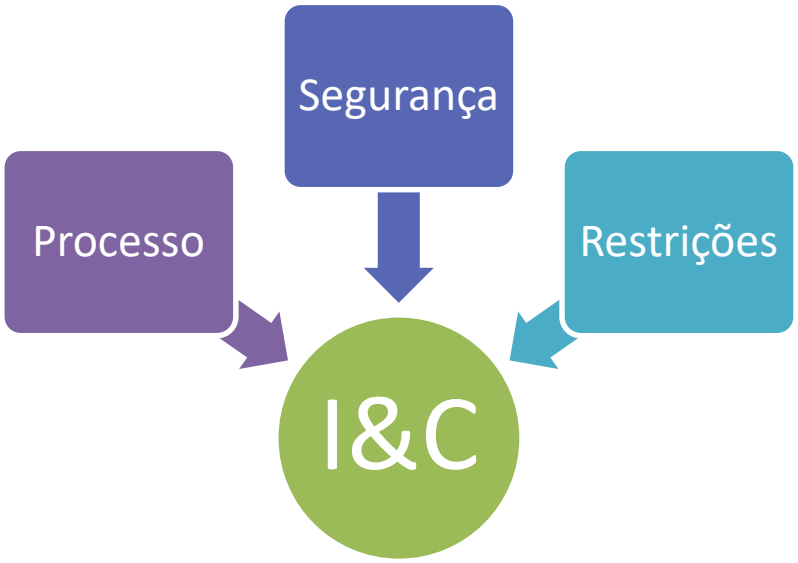
No que tange a especificação de requisitos, o conjunto dos princípios e critérios da base normativa nuclear, juntados a eles os requisitos de cunho mais funcional e de restrições de projeto formam a base dos requisitos de projeto. Este conjunto de requisitos visa cumprir a estratégia de redução de riscos assumida pelos atores de alto nível do empreendimento (clientes e arquiteto geral).

No caso específico dos sistemas de I&C serão desenhadas estratégias específicas, que obviamente tem sua base amparada na estratégia de alto nível refletida nas declinações dos níveis superiores de especificação. Podemos citar como exemplo estratégias de falha segura em caso de perda de energia. Portanto, a estratégia dos sistemas

de I&C, originadas em uma estratégia global, formarão os critérios gerais de projeto para sistemas de I&C que darão base para o plano tecnológico a ser incorporado no projeto.

Os critérios gerais de projeto de I&C deverão atender três grandes grupos de especificações de requisitos: de processo, de segurança, e as restrições de projeto (Figura 7). Os requisitos de processo são aqueles especificados pelas EPUNM contendo as especificações operacionais dos sistemas da UNM que precisam ser controladas. Os requisitos de segurança são aqueles requisitos impostos de forma transversa pelo time de segurança para se garantir os princípios de segurança nuclear da planta. Os requisitos de restrição de projeto são aqueles impostos pelos times de estruturas, arranjo, logística, e qualidade para garantir a viabilidade do projeto dentro das limitações de construção da UNM (SUMMERS, 2007).

Figura 7 - Categorias de requisitos que impactam projetos de Sistemas de I&C

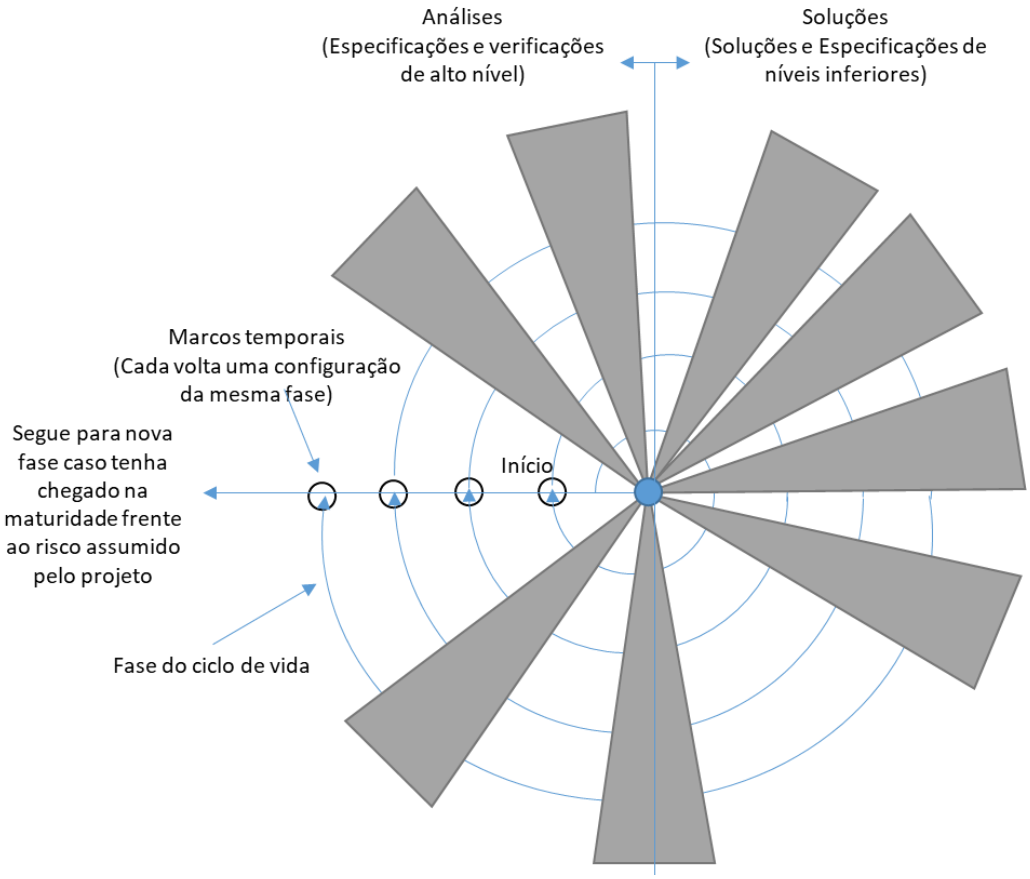


Posteriormente, com a primeira configuração de projeto será possível realizar um balanço de segurança nuclear, avaliando a aderência aos princípios de segurança nuclear. Este balanço pode ser realizado pelas equipes de segurança e licenciamento (do projeto ou empreendimento), sendo uma revisão interna predecessora a uma possível revisão pelo órgão regulador. Esta avaliação pode ser feita a partir de matrizes de verificação de atendimento aos requisitos, assumindo-se critérios para se estabelecer o grau de maturidade do projeto e aderência aos princípios de segurança nuclear.

Esse grau de maturidade é medido e caracterizado por uma "*Functional Baseline*". A fase de projeto básico deve dar os subsídios necessários, dentro de um projeto preliminar e de completação tecnológica. Ou seja, deve ser possível realizar um balanço geral e avaliar os riscos de se empreender o projeto. Esta avaliação irá verificar se o projeto está suficientemente detalhado (conforme a linha base prevista) para que se atendam às necessidades requisitadas pelo cliente final (NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, 2007).

Como podemos ver na figura 8, dentro das fases específicas do ciclo V pode-se utilizar o processo em espiral. A intenção é implementar uma fase de projeto repetidas vezes, classificadas em diferentes configurações, por exemplo: Fase de Projeto Básico – Configuração A, ou B, ou C, etc. Esta abordagem permite a execução de balanços de projeto em respectivos marcos temporais para verificar se o projeto já estaria maduro, ou consistentemente viável para passar para uma grande fase de projeto subsequente.

Figura 8 - Modelo espiral de processo de projetos



Fonte: adaptado de TOMMILA, 2016.

Como se pode notar na figura 8, o processo em espiral é dividido em dois grandes domínios, um analítico e outro de solução. A ideia apresentada é a de que as soluções são geradas a partir de atividades analíticas:

- Inicia-se o domínio de análise: determinam-se contextos e atores envolvidos, as necessidades e restrições do cliente e do projeto;
- Passa-se ao domínio de soluções: definem-se os sistemas, alocam-se as respectivas funções, estabelecem-se os *layouts* e arquiteturas, avaliam-se os cenários a partir dos binômios: causa e consequência, estabelecem-se os requisitos de projeto;
- Volta-se ao domínio de análise: onde se realizam as avaliações e balanços gerais, estabelecem-se e reajustam-se os planejamentos do projeto.

Claro que a figura é sucinta, e não relaciona todas as atividades de forma exaustiva. As verificações precisam de parâmetros claros para validar ou não o atendimento de um requisito por uma solução técnica em nível de sistemas ou equipamentos. Outro item a ser levado em consideração na base do projeto para as especificações dos requisitos são os fatores e desafios considerados para a operação da planta. Os engenheiros de processo, juntamente com os engenheiros dos sistemas de I&C, conjuntamente com os potenciais operadores e equipes de manutenção, que devem levantar tais requisitos mais ligados à operação da planta.

Estas estratégias de verificação, de operabilidade e manutenibilidade devem estar estabelecidas conjuntamente com as especificações dos requisitos, para que não se prejudique o andamento real do projeto. Ou seja, os requisitos (principalmente aqueles que compõem as especificações nos níveis de sistemas e equipamentos) precisam ser do tipo SMART ("*specific, measurable, achievable, realistic, traceable*"). Isso, para evitar más interpretações das especificações e garantir a rastreabilidade na subida do ciclo V quando da verificação.

2.5 Sistemas I&C e a importância para a segurança nuclear

Os sistemas de I&C, devido a sua importância dentro de uma UNM, possuem estreita relação com critérios de segurança nuclear. Como bem alertado por FREIRE (2018), conclui-se que devido o gigantismo de um empreendimento nuclear, qualquer

falha pode levar a elevados riscos. Risco estes que podem ser de natureza financeira, ou a outros até mais preocupantes, como riscos à segurança de pessoas e ao meio ambiente.

Dentro do universo de sistemas de I&C, os Sistemas de Proteção, ou genericamente Sistemas Instrumentados de Segurança (SIS), são aqueles compostos por sensores, controladores (solucionadores de lógicas) e elementos finais de controle (atuadores) que visam levar ou manter um processo em condições seguras antes, durante e depois de acidentes, quando valores predeterminados ("*set points*") são excedidos.

Outros sistemas de I&C que não tem relação direta com a função de proteção, mas que também controlam parâmetros relacionados com as barreiras físicas de proteção, também recebem requisitos que abarcam propósitos relacionados à segurança nuclear, mesmo que indiretamente. Estes direcionamentos serão explorados ao longo do trabalho, em torno principalmente da estratégia de Defesa em Profundidade (DiD).

Em suma, sistemas de I&C que são classificados dentro de uma análise de segurança como possuindo uma função de serviço categorizada como de segurança nuclear, ou que seu mau funcionamento ou falha podem levar a exposição à radiação trabalhadores da UNM ou ao público como um todo, são sistemas de I&C com Função Importante para Segurança Nuclear (FIS).

Alguns exemplos desses sistemas seriam: Sistema de Proteção do Reator; Sistema de Controle do Reator; Sistema de Controle e Monitoramento de Reatividade; Sistema de Controle e Monitoramento de Resfriamento do Núcleo; Sistema de Controle e Monitoramento do Fornecimento de Energia de Emergência; Sistema de Isolamento da Contenção; Sistema de Monitoramento Pós-Acidental; Sistema para Monitoramento de Efluentes, Sistema para Manuseio do Elemento Combustível, dentre outros (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016).

2.6 Sistemas I&C e as principais bases normativas

Foi levantado na literatura acadêmica nacional e internacional conceitos e teorias da lei construtal para identificação da taxonomia utilizada nas diversas metodologias como forma de facilitação do fluxo de informações. A partir da pesquisa inicial das normas ou regras de classificação das entidades de dados, constataram-se as estratégias utilizadas na relação e parametrização dos metadados gerados, métodos de consulta e monitoramento das interfaces e fluxo de dados das diversas metodologias.

As principais bases normativas utilizadas internacionalmente são a U.S. NRC (americana) e a IAEA (internacional). Dentro dessas bases, duas foram as formas de aplicação da relação segurança frente ao custo. Na revisão bibliográfica as abordagens aplicadas eram a ALARA (*"as low as reasonably achievable*"), e ALARP (*"as low as reasonably practicable"*). A distinção entre as duas na aplicação aos sistemas de I&C refere-se principalmente ao fato da flexibilização do projeto e sua demonstração NUCLEAR REGULATORY COMMISSION, 2020a; INTERNATIONAL ATOMIC ENERGY AGENCY, 2012).

A análise de custo-benefício dentro das bases normativas leva em consideração técnicas sistemáticas de avaliação dos benefícios e malefícios na condução do projeto. ALARP leva em consideração uma otimização dos sistemas de segurança com vistas principalmente à segurança. ALARP, entretanto define os critérios nas zonas de risco mais insignificantes.

Segundo a CFR:

> *ALARA is an acronym for "as low as (is) reasonably achievable," which means making every reasonable effort to maintain exposures to ionizing radiation as far below the dose limits as practical, consistent with the purpose for which the licensed activity is undertaken, taking into account the state of technology, the economics of improvements in relation to state of technology, the economics of improvements in relation to benefits to the public health and safety, and other societal and socioeconomic considerations, and in relation to utilization of nuclear energy and licensed materials in the public interest.* (NUCLEAR REGULATORY COMMISSION, 2020a).

Segundo a IAEA, ALARP é:

> *The philosophy of dealing with risks that fall between an upper and lower extreme. The upper extreme is where the risk is so great that it is rejected completely while the lower extreme is where the risk is, or has been made to be, insignificant. This philosophy considers both the costs and benefits of risk reduction to make the risk "as low as reasonably practicable*. (INTERNATIONAL ATOMIC ENERGY AGENCY, 2012)

Neste ínterim, a evolução dos guias de projeto ou ciclos de vida de um empreendimento perseguiu estas condições de riscos, segurança e custo. Foram desenvolvidos métodos de gerenciamento de projetos, tais como: PMBOK (PMI); "*Safety Guides*" (IAEA ou NUREG); "*Standards*" (ISO/IEC); "*Engineering Handbook*" da NASA e outros. Algumas normas específicas referem-se ao ciclo de vida de um projeto

de I&C, e devido à complexidade ao desenvolvimento de hardware e software, estas normas abordam com maior clareza cada etapa necessária.

Realizando um comparativo entre a base normativa nuclear americana (U.S. NRC) e europeia (IAEA), verificou-se que a IAEA estabelece uma estruturação normativa de cima para baixo com maior clareza. Nota-se que primeiro tem-se a IAEA SSR-2/1 (*Safety of nuclear power plants: Design*), onde são especificados os requisitos de segurança nucleares de mais alto nível.

Depois tem-se a IAEA SSG-30 (*Safety Classification of Structures, Systems and Components in Nuclear Power Plants*), onde são estabelecidos os critérios gerais e métodos de classificação nuclear de itens de uma UNM. Depois tem-se a IAEA SSG-39 (*Design of instrumentation and control systems for nuclear power plants*), que é o documento que estabelece as entradas e saídas de todo o ciclo de vida de um projeto de sistemas de I&C, e soma-se a esta, a IAEA SSG-51 (*Human factors engineering in the design of nuclear power plants National regulations*) que estabelece todo o programa de engenharia de fatores humanos a ser executado.

Isso não quer dizer que a base normativa americana (U.S.NRC) não possua tal organização. No painel "Regulatory Guidance Framework for IEEE Standards – P61226" é exposto com clareza o concatenamento dos guias do órgão regulador (*Regulatory Guides* - RG) e respectivos endossos à norma industrial da IEEE. Partindo deste concatenamento, a WNA estabeleceu uma correlação das bases normativa europeia e americana. A tabela 1 apresenta alguns exemplos desta correlação entre a base americana e internacional (WORLD NUCLEAR ASSOCIATION, 2020).

Tabela 1 - Exemplos de normas que se referem a sistemas I&C

Base Americana		**Base Internacional**	**Objetivo**
P61226 Categorization and classification of I&C and electrical systems		IEC 61226:2019 Classification of instrumentation and control functions	Estabelecimento de métodos de classificação dos itens e funções de controle nucleares.
Reg guide 1.201 2006 Guidelines for categorizing systems, structures, and components according to safety significance	IEEE 1819™-2016 Risk-informed categorization of electrical and electronic equipment	IEC TR 61838:2009 Use of probabilistic safety assessment for the classification of functions	Avaliações de risco para categorização e classificação das funções de controle e/ou componentes/sistemas.

Base Americana		Base Internacional	Objetivo
Reg Guide 1.75 2005 Criteria for independence of electrical safety systems	IEEE 384™-2018 Independence of 1E equipment and circuits	IEC 60709:2018 Separation	Aplicação de critérios e técnicas para aumentar o nível de tolerância a falhas dos sistemas de I&C.
Reg Guide 1.53 2003 Application of the single-failure criterion	IEEE 379™-2014 Application of the single failure criterion	-	Aplicação de critérios e técnicas de análise de falhas simples para aumento da robustez e confiabilidade de sistemas de segurança de geração de energia elétrica.
Reg Guide 1.22 1972 Periodic testing of protection system actuation functions	IEEE 338™-2012 Criteria for periodic surveillance testing	IEC 60671:2007 Surveillance testing	Critérios de testes e procedimentos de inspeção dos sistemas de I&C.
Reg Guide 1.118 1995 Periodic testing of electric power and protection systems			
-	-	IEC 62340:2007 Requirements for coping with common cause failure	Técnicas para evitar modos de falha comum em equipamentos diversos e/ou redundantes.

Fonte: adaptado de WORLD NUCLEAR ASSOCIATION, 2020.

Com toda essa revisão bibliográfica, expôs-se a necessidade de metodologias mais claras que mitiguem os riscos em projetos de I&C. Isto se deve em parte ao tamanho das usinas nucleares, aos seus estudos de viabilidade, à magnitude dos investimentos nucleares, às formas de se mensurar os erros de projeto em termos de prejuízo financeiro e ambiental, ou ainda expondo a complexidade dos sistemas I&C. Com isso foi possível confrontar os tipos de metodologias em sua classificação mais ampla. Ou seja, um projeto baseado em validação de documentação ("*document-based*"), ou um projeto baseado na validação de uma base de dados ("*model-based*").

Em sistemas complexos, como uma planta nuclear embarcada, o melhor caminho seria o projeto "*model-based*" (NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, 2007; FREIRE, 2018). Este projeto é implementado através de técnicas e ferramentas de Gerenciamento de Engenharia de Sistemas (*System Engineering Management*). Estas ferramentas permitem maximizar o sucesso de projetos de sistemas complexos, provendo métodos efetivos para gerenciamento de requisitos e interfaces, e definindo o escopo de cada ator dentro projeto. Algumas normas que tratam sobre o assunto são a EIA-632 (ELECTRONIC INDUSTRIES ALLIANCE, 2019), IEEE 1220

(IEEE POWER ENGINEERING, 2005) e ISO/IEC 15228 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION and THE INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2001).

Alguns exemplos de metodologias de projeto de sistemas são o "Processo Harmony SE" e "RUP SE" desenvolvido pela IBM, o "*State analysis*" do "*Jet propulsion laboratory*" da NASA, a Metodologia Strata da Vitech, o "*Lifecycle Modeling Language Specification*" do LML comitee. Todas teoricamente permitiriam a aplicação de projeto para sistemas de I&C.

Exemplos de ferramentas que poderiam aplicar estas modelagens são: Innoslate (SPEC Innovations); NIMA – NASA Integrated Model-centric Architeture; OOSE (OMG); Craddle; Smart Plant Instrumentation (SPI); e COMOS. Contudo, apenas as duas últimas opções pesquisadas são específicas de sistemas de I&C, e em tese poderiam atender as hipóteses lançadas por este trabalho, mas não em sua plenitude por serem ferramentas típicas para as fases de projeto executivo.

3 METODOLOGIA

Este capítulo apresenta os métodos empregados para que os objetivos propostos por esse trabalho sejam atingidos.

3.1 Tipo de estudo

O desenvolvimento deste trabalho é inteiramente conceitual e não envolve experimentos. A pesquisa foi conduzida seguindo um estudo descritivo e exploratório, que se respaldou, em um primeiro momento, em uma pesquisa bibliográfica para fundamentação, análise e discussão do tema em questão. O estudo foi descritivo pois buscou observar, registrar, analisar e correlacionar fatos, e em seguida exploratório para permitir um auxílio no levantamento de hipóteses (LEOCARDIO, 2020).

3.2 Delineamento da pesquisa

O ponto de partida foi a tese defendia por FREIRE (2018), onde é afirmado que:

> *Para facilitar os fluxos de informação, essa tese define conceitos estendendo a engenharia de sistemas e demonstra a utilidade da aplicação de tais conceitos em um projeto. Tal aplicação leva a uma série de requisitos a serem considerados durante o projeto de sistemas, requisitos esses que são justificados à luz da lei construtal. Esta tese aplica esses requisitos a uma pessoa de uma equipe de projeto e propõe um método de desenvolvimento de sistemas.* (FREIRE, 2018).

Para delinear objetivamente o trabalho, e garantir uma adequabilidade aos conceitos da lei construtal desenvolvida na tese de FREIRE (2018), foram tabeladas as hipóteses e respectivas descrições (com sucintas adaptações), conforme apresentado na tabela 2. Os conceitos foram relacionados aos seus propósitos, requisitos e relevância. O método visará garantir que as hipóteses 2 e 3 serão aplicadas e atendidas de forma transversal pela metodologia de especificação de sistemas de I&C deste trabalho. As demais hipóteses estarão implicitamente aplicadas nos modelos (*templates*) apresentados no anexo 4.

Tabela 2 - Hipóteses para atendimento à Lei Construtal

Hipótese	**Descrição**	**Relevância** (Essencial para)	**Propósito** (Necessário para)	**Requisito** (Necessita de)
1	Um dos principais fluxos institucionais é a informação.	- Que as pessoas (atores envolvidos) ajam conforme as necessidades de outros. - Produzir trabalho com eficiência e foco.	- Tomadas de decisão.	- Protocolo (linguagem) comum ao emissor (cliente) e receptor (provedor). - Meio físico (canal) de transmissão.
2	Para assegurar a passagem de fluxos o canal precisa facilitar o escoamento, reduzir a contaminação e preservar a integridade.	- Comunicação. - Trocas de fluxos. *	- A ocorrência de fluxos.	- Meios para facilitar o escoamento. - Meios para reduzir a contaminação. - Meios para preservar a integridade do fluxo.
3	Maximização dos fluxos com menor custo esperado na curva total versus segurança.	- Tornar o sistema viável.	- Redução de ruídos - Garantia da integridade da informação.	- Atingir um ponto ótimo onde o investimento em segurança torna a solução mais eficiente. **
4	Necessidade de operar em malha fechada.	- Garantir os objetivos do processo.	- Monitoração de ruído e das perturbações sistêmicas.	- Meios para medição das variáveis do processo. - Interfaces de comando. - Reportar o estado do sistema.
5	Assumir que a ignorância do autor da especificação sobre o estado da arte e melhor capacidade do fornecedor.	- Garantir a simetria da informação. - Garantir a viabilidade do projeto.	- Delimitação do escopo de funções dos entes do projeto.	- Procedimentos claros para elaboração e alcance das especificações
6	Assumir que especificações inviáveis representam um perigo.	- Evitar prejuízos - Optimização do tempo. - Garantir a viabilidade do projeto.	- Elaboração de especificações técnicas realistas e viáveis.	- Prover meios de trocas de informação entre potenciais fornecedores, clientes e arquitetos.
7	Separação formal entre necessidades e soluções técnicas.	- Preservar a liberdade do projetista. - Garantir a separação formal entre problema (necessidade) e solução (produto).	- Enuncia as necessidades a serem satisfeitas pelo sistema. ***	- Não definir a solução técnica. - Não fazer menção à arquitetura física.

Fonte: adaptado de FREIRE (2018).

Notas:

** Para maiores detalhes consultar FREIRE (2018) – fig. 12;*

*** Para maiores detalhes consultar FREIRE (2018) – fig. 13;*

**** Para maiores detalhes consultar FREIRE (2018) – fig. 14;*

No intuito de harmonizar a terminologia utilizada nas especificações de sistemas de I&C frente à metodologia desenvolvida na tese de FREIRE (2018), foi elaborado o anexo 1 (Terminologias e conceitos relativos à engenharia de sistema) onde foram tabelados os conceitos da tese citada (com sucintas adaptações), e adicionadas as correlações entre os diversos conceitos. Outros conceitos não catalogados na tese de FREIRE (2018) foram complementados para sustentar este trabalho.

Este estudo visa definir o escopo de trabalho de uma equipe de controle no projeto básico (especificações mínimas) e justificá-los de acordo com a lei construtal (Tabela 2). Para isso, serão propostos: o modo de levantamento do conjunto de normas que norteiam o trabalho de I&C (lista de normas e sua aplicabilidade); o modo para concepção da arquitetura geral e alocações de volume, peso, consumo elétrico e requisitos não funcionais (descritivo de sistema de controle); o modo para catalogação das funções de controle de acordo com os níveis de segurança; modo para alocação das arquiteturas de I&C, para permitir a produção de especificações funcionais e de interface.

3.3 Embasamento teórico

A definição do escopo, através de descritivos e modelos, facilitará a especificação dos sistemas I&C compreendidos no projeto básico. Ou seja: a organização destes sistemas, a alocação das funções de I&C destes sistemas, a interconexão entre os sistemas (definindo as interações alocadas), as restrições de projeto (incluindo as interações proibidas e o comportamento desejável alocado na arquitetura geral), e as definições das fronteiras entre os diversos sistemas (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016).

Em suma, a pesquisa realizada levou às seguintes atividades de projeto, de forma horizontal (transversa – generalista e que gera requisitos para todos os sistemas da UNM que tem relação com I&C) e vertical (interna – específica dos sistemas de controle):

1) Especificação dos critérios gerais de I&C - horizontal:
    a. Escopo funcional ou Categorização funcional em termos de controle: Trata-se de uma especificação integrante dos “Princípios da UNM”, onde há o estabelecimento dos escopos de controle e proteção da planta. Organização a nível de planta, definindo quais categorias funcionais serão controladas pelos sistemas de controle normal e de segurança da planta.

b. Meios de operação: Trata-se de uma especificação integrante dos "Princípios da UNM", onde há o estabelecimento dos meios disponíveis de controle, monitoramento e operação manual da planta. Estes critérios deverão ser declinados como restrições de projeto dos níveis superiores aos níveis inferiores.
c. Plano tecnológico de I&C: Trata-se de uma especificação integrante dos "Princípios da UNM", onde há a definição da instrumentação a ser utilizada como base para a especificação dos diversos sistemas da planta que possuem relação com os sistemas de I&C.

2) Especificação das arquiteturas funcionais - horizontal:
   a. Declinação funcional e classificação: Baseada numa arquitetura DiD (funcional). Trata-se da distribuição das funções da UNM em conformidade com a categorização dos eventos ou estados da planta em blocos funcionais, determinando onde serão implementadas as funções de controle ("*control functions*"). Nestes blocos estarão as funções de cada sistema de I&C (funções de controle definidas em nível macro pelo AGUNM que especifica os princípios de operação da planta), e as funções a serem controladas. Todas as demandas devem ser claramente identificadas no projeto, para facilitação do fluxo de informações entre os atores envolvidos – Sistemas, Estruturas, Componentes (SSCs) das EPUNM, e a equipe de controle - ECUNM;
   b. Interfaces funcionais e condições da planta: Identificar as interfaces funcionais ("*functional links*") de cada bloco de função, para permitir a avaliação da diversidade funcional. A definição das interfaces funcionais deve visar a determinação dos dados (protocolo e fluxo de sinal) trocados entre as diversas funções da UNM (nível macro, a partir das definições do AGUNM). Neste passo a estratégia é a utilização da defesa em profundidade – Arquitetura DiD.
   c. Arquitetura geral de automação (funcional): Estabelecimento de uma arquitetura geral de I&C com base nas camadas ("*layers*") de automação industrial (sensores e atuadores, dispositivos controladores de campo, sistemas de controle de processo, sistema de supervisório e de informações, e sistema de gerenciamento de informações técnicas).

3) Especificação das arquiteturas típicas - horizontal:
    a. Malhas de I&C: Especificação das malhas de I&C e suas classificações conforme as funções da planta e as funções de controle ("*control functions*") estabelecidas pelas EPUNM;
    b. Arquiteturas típicas: Elaboração e catalogação de arquiteturas típicas de controle para atendimento à UNM como um todo, buscando-se assim a padronização da filosofia de I&C para o monitoramento e controle das SCCs;
    c. Alocação das malhas de I&C: Catalogação e alocação das malhas de I&C, adotando os critérios de DiD ou D3 previstos, e direcionamento/alocação à arquitetura típica específica;
    d. Relatório de Entrada e Saída (ES) e de Funções de Controle (FC): Geração de relatórios de entrada e saída (I/O) e diagramas de malhas de I&C. Relatórios apresentados em formas de "*templates"* para permitir a avaliação a nível global da UNM, ou a nível de detalhamento.
4) Especificação dos Sistemas de Controle - vertical:
    a. Descritivos de Sistema: Elaboração de uma especificação de Sistemas de I&C, onde conste descrição sumária do sistema, com análise funcional e requisitos, definição de interfaces, arquitetura física, lista de componentes, e considerações de arranjo;
    b. Caracterização do Sistema: Descrição funcional do sistema, dos componentes, balanços de peso, balanços de consumo elétrico, balanços térmicos, balanços de volume requeridos, requisitos não funcionais – ambiental, segurança, HFE, segurança cibernética, compatibilidade eletromagnética, manutenibilidade, construtibilidade etc.;
    c. Operação do sistema: Descrição de operação do sistema com as configurações de operação, diagrama de estados, descrição dos estados e transições. Na especificação devem-se definir as necessidades de funções de controle e monitoramento a partir das transições, alocação das necessidades aos meios de controle e monitoramento disponíveis, arquitetura de controle e supervisório.

Com o propósito de evidenciar que os objetivos estabelecidos no item 1.1 deste trabalho foram atingidos, foi realizada a verificação das hipóteses deste trabalho frente à tese de FREIRE (2018). A tabela 3 apresenta esta relação.

Tabela 3 - Atividades vs. Hipóteses da Lei Construtal

Atividades de especificação de sistemas de I&C		Hipóteses Freire							Justificativa
		1	2	3	4	5	6	7	
1.a	Critérios gerais de I&C: Escopo funcional	X	X	X	-	-	-	X	Os critérios gerais tomam a decisão da troca das informações, preservando assim a integridade com vistas gerais a viabilidade do projeto.
1.b	Critérios gerais de I&C: Meios de operação	X	X	X	-	-	-	-	
1.c	Critérios gerais de I&C: Plano tecnológico	X	X	X	-	X	X	-	
2.a	Arquiteturas funcionais: Declinação funcional e classificação	X	X	X	-	-	-	X	As arquiteturas funcionais não devem adentrar na solução técnica do projetista, contudo devem garantir que os critérios gerais cheguem aos projetistas.
2.b	Arquiteturas funcionais: Interfaces funcionais e condições da planta	X	X	X	-	-	-	X	
2.c	Arquiteturas funcionais: Arquitetura global e interfaces	X	X	X	-	-	-	X	
3.a	Arquiteturas típicas: Malhas de I&C	X	X	X	X	-	-	-	As arquiteturas típicas já estabelecem uma solução técnica, levando em consideração às necessidades dos projetistas com vistas aos critérios gerais.
3.b	Arquiteturas típicas: típicos	X	X	X	X	-	-	-	
3.c	Arquiteturas típicas: Alocação das malhas de I&C	X	X	X	X	-	-	-	
3.d	Arquiteturas típicas: Relatórios	X	X	X	X	-	-	-	
4.a	Especificação de sistemas de controle: Descrição	X	X	X	-	X	X	-	As especificações detalham a solução técnica, a partir do declínio dos requisitos dos níveis superiores.
4.b	Especificação de sistemas de controle: Caracterização	X	X	X	-	X	X	-	
4.c	Especificação de sistemas de controle: Operação	X	X	X	X	X	X	-	

3.4 Desenvolvimento da metodologia

3.4.1 Levantamento de requisitos metodológicos para a especificação de sistemas de I&C de usina nuclear móvel

Essa atividade responde as seguintes questões: quem são os atores envolvidos? Quais as atribuições de cada ator e sua posição no empreendimento da organização industrial? Quais os entregáveis de cada atividade e a quem eles serão reportados? Quais as normas nucleares aplicáveis para cada atividade? Quais as orientações metodológicas existentes em normas?

Ao pesquisar respostas a estes questionamentos, foi possível tocar nos diversos temas concernentes aos sistemas I&C. Devido à complexidade dos sistemas I&C, não há como negar a contribuição dos vários pontos de vista oriundos de outras disciplinas

correlacionadas. Para isso uma metodologia de gestão destas informações, transparecendo a todos os envolvidos a forma atual do estágio do projeto se torna fundamental.

Tocando nestes quesitos, e assim identificando claramente os atores, atribuições de cada um, os entregáveis e a quem serão reportados, quais normas nucleares envolvidas e a filosofia utilizada, evitar-se-á que as soluções definidas pelo engenheiro de processo ou mecânico sejam fixadas antes do envolvimento dos engenheiros de I&C (problemas recorrentes em projetos). Ainda há a necessidade da integração entre o programa de "*Human Factors Engineering*" (HFE) e de "*Cyber Security*" mais as soluções dos projetistas dos sistemas (INTERNATIONAL ATOMIC ENERGY AGENCY, 2016).

Para se chegar a estes requisitos e garantir a preservação das hipóteses supracitadas sobre a adequabilidade à lei construtal, foram utilizados os requisitos do anexo 1 da tese de FREIRE (2018) como base para o levantamento das etapas de especificação propostas neste trabalho. Para manter a rastreabilidade dos requisitos, a tabela 9 apresenta a numeração do item do requisito na ordem apresentada por FREIRE (2018). A ordem de atividades proposta pela linha metodológica deste trabalho não é a mesma do ordenamento dos requisitos.

3.4.2 Proposição da linha metodologia

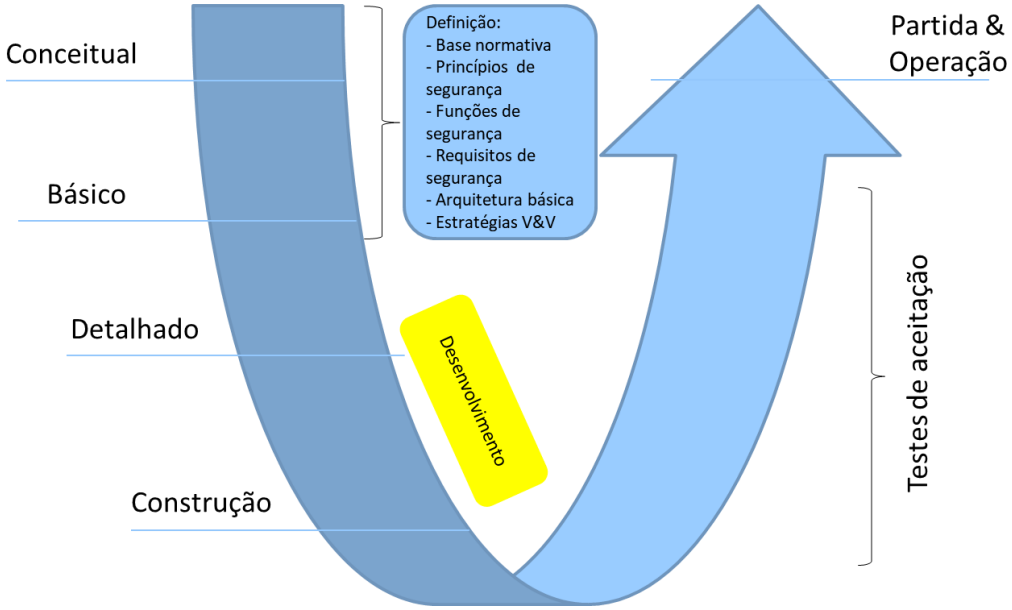
Essa atividade responde as seguintes questões: qual a sequência das atividades por ator? Quais os requisitos de cada entregável? Como verificar o cumprimento dos requisitos? Como evitar o surgimento de conflitos entre atores? Como solucionar conflitos entre atores? Como motivar os atores? Quais os requisitos técnicos aplicáveis ao caso particular?

Para responder a essas questões, cabe de fato aprofundar na definição dos elementos que configurariam as bases do projeto. Conceitos de operação e controle deverão ser utilizados nas diversas instalações a serem controladas. Devido à interdisciplinaridade destes tipos de projetos, as descrições de operação e controle são sempre definidas pelos diversos atores envolvidos. Num projeto nuclear conceitos de "*Functions Important to Safety*" (FIS), "*Nuclear Safety Classification*" (NSC), "*Defence in Depth*" (DiD) são exemplos de termos que deverão estar claros e alinhados com os "*Operation Concepts*" (OpC) quando da definição das funções e seu declínio do alto nível aos níveis mais baixos.

Em suma, a linha metodológica tem como eixo central uma abordagem metodológica que, a partir de uma análise funcional com vistas à classificação de segurança nuclear, permita a definição dos requisitos básicos de projeto para a especificação de sistemas de I&C. Proposição de temas capitais, no que tange a classificação de segurança também devem ser delineados, tais como: metodologia de segurança, base de projeto, análise funcional, especificação de requisitos e viabilização de um processo de obtenção.

De forma simplificada, a figura 9 apresenta o ciclo de vida em V com as grandes fases de um projeto: conceitual, básico e detalhamento. Como já mencionado anteriormente, este trabalho foi delimitado na fase de projeto básico.

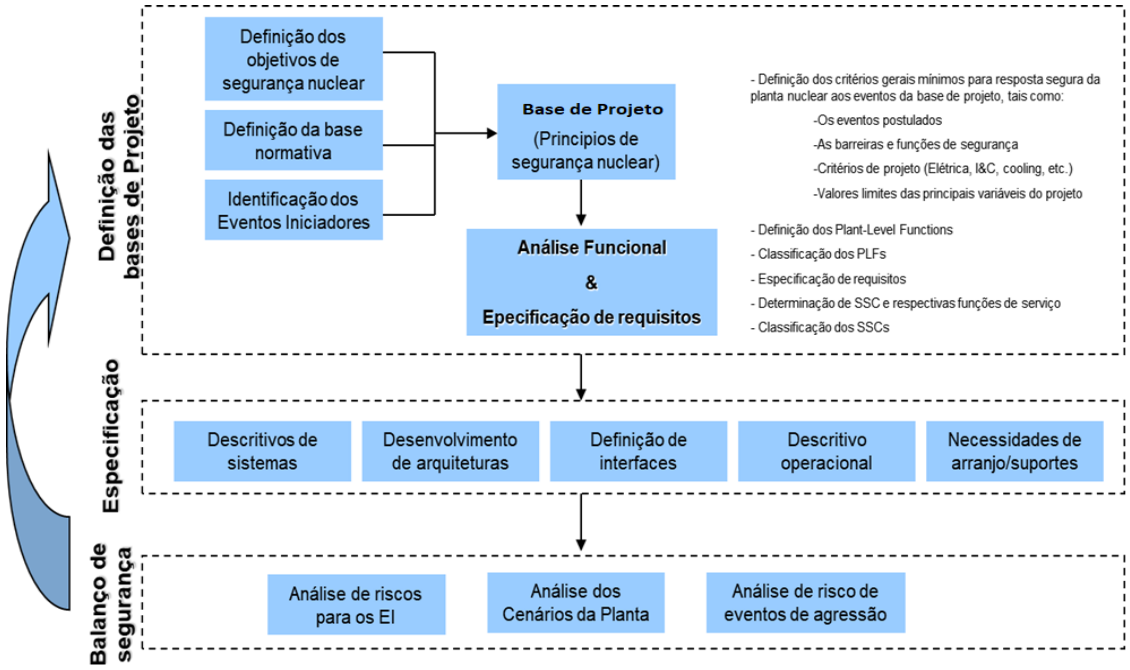
Figura 9 - Ciclo de Vida em V simplificado e respectivas fases



Este trabalho propõe uma demarcação das atividades de I&C necessárias frente aos objetivos de segurança nuclear (bases de projeto e análise). Portanto para se definir a sequência das atividades por ator e os entregáveis de cada um, foi necessário delimitar três subfases dentro de uma fase de projeto.

Lembra-se que estas subfases seriam compostas por entregáveis (documentos ou dados) elaborados pela equipe de projeto com contribuições das equipes de segurança e licenciamento, principalmente naqueles que definem a base de projeto e que realizam o balanço de segurança nuclear. A figura 10 apresenta essa macrovisão das subfases do projeto.

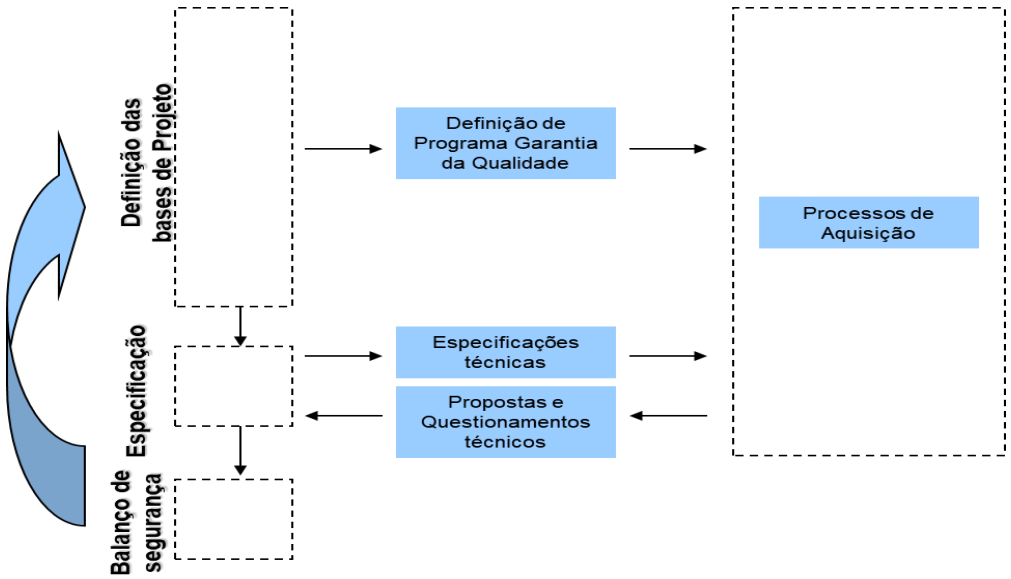
Figura 10 - Macrovisão da fase do projeto básico



Os entregáveis utilizados no balanço de segurança não são focos deste trabalho. Este trabalho buscará atender as necessidades do nível de especificação, tendo que adentrar nos limites da definição das bases de projeto fornecendo os critérios gerais de I&C, e das especificações propriamente ditas.

Devido à grande ingerência do processo de obtenção dentro da especificação, este trabalho também avaliou de forma básica as interfaces com os entregáveis relacionados à obtenção dos SSCs. Na figura 11 é possível notar tais interfaces.

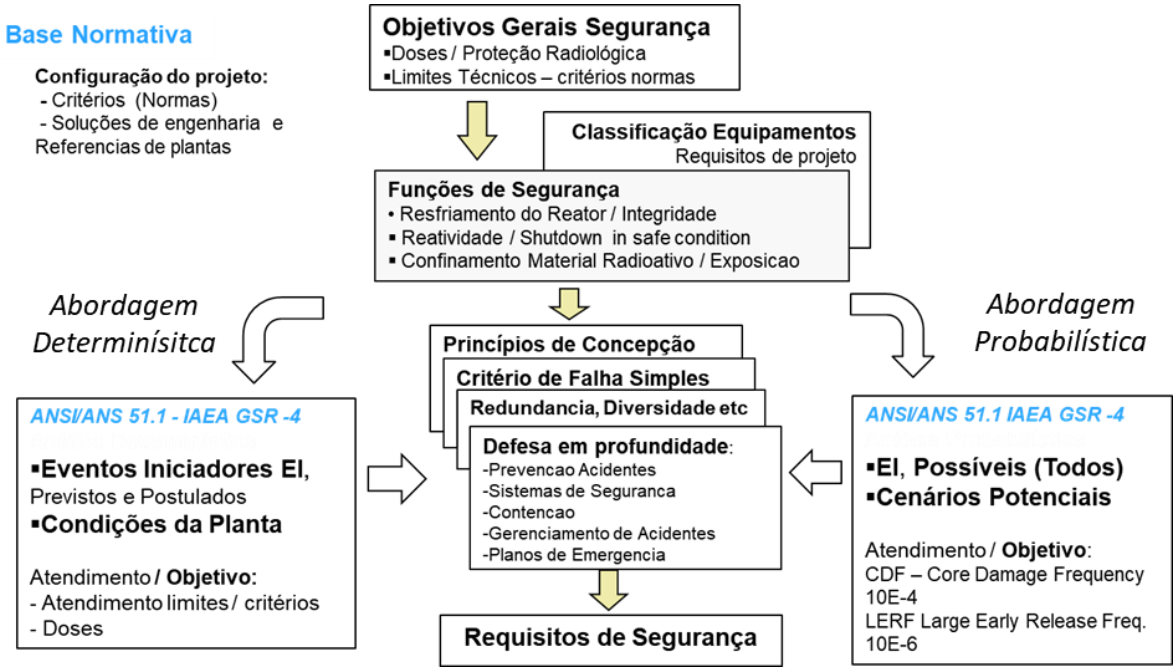
Figura 11 - Macrovisão das interfaces entre o projeto e a obtenção



A figura 12 contempla o universo do projeto em conjunto com a definição das Bases de Projeto, que responderiam aos quesitos de verificação do cumprimento dos requisitos de cada entregável, o que evitaria o surgimento de conflitos entre os atores. Traçou-se desse modo a base para metodologia deste trabalho, tanto na definição da base normativa ou dos princípios nucleares.

A metodologia deste trabalho será delimitada pela base normativa nuclear americana, visto que Comissão Nacional de Energia Nuclear (CNEN) foi fortemente influenciada pelo modelo de licenciamento da U.S. NRC (FRUTUOSO et al, 2011). Além disso, a vantagem do uso desta base são as publicações da U.S.NRC que tratam com profundidade o programa de HFE, que influencia sensivelmente as especificações de sistemas de I&C (AVELLAR e SCHIRRU, 2019). Todavia, a base normativa é aplicável a uma planta nuclear de terra. Portanto algumas referências serão readequadas, retiradas, e direcionadas a outros organismos, principalmente a IAEA.

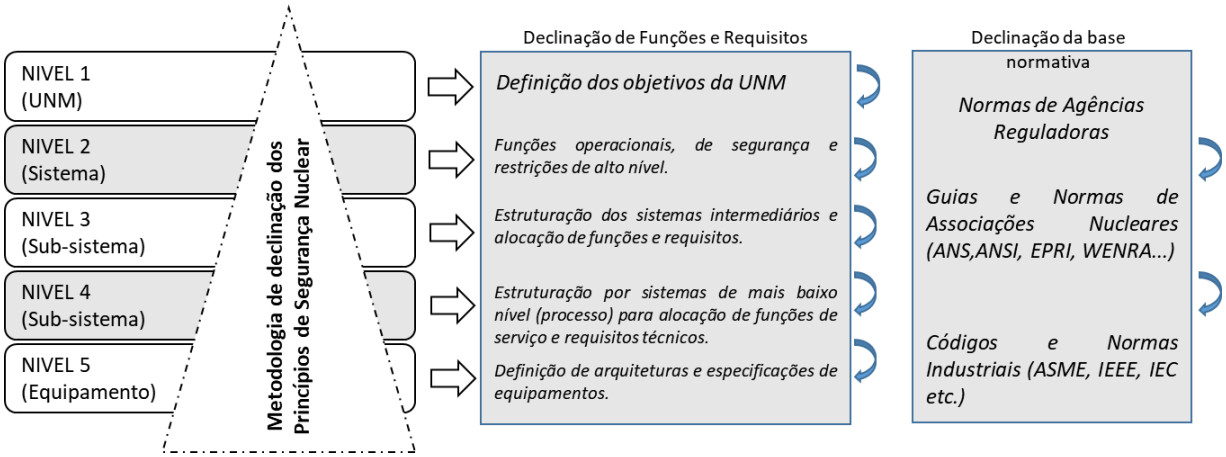
Figura 12 - Macrovisão da base metodológica para segurança nuclear



A figura 13 orienta de modo sucinto toda a metodologia de declinação assumida neste trabalho. A estratégia de cima para baixo dos princípios de segurança nuclear, deve ser tal que clarifique a todos os atores a declinação funcional e dos requisitos, com o evidente declínio da base normativa. Desta forma, em cada nível de responsabilidades, os

atores poderão constatar a fonte das funções e requisitos que lhe foram atribuídos. Essa forma de estratégia garante a motivação e engajamento do grupo de trabalho.

Figura 13 - Estratégia “de cima para baixo” dos princípios de segurança nuclear



3.4.3 Proposição de implementação da linha metodológica

Seguindo a linha metodológica do trabalho é possível identificar que para a especificação de um sistema de I&C são necessários no mínimo os seguintes itens:

1) Critérios gerais de I&C (Especificação de requisitos transversos):
   a) Delimitação do escopo funcional dos Sistemas de I&C;
   b) Especificação dos meios disponíveis de operação; e
   c) Especificação do plano tecnológico de I&C.
2) Arquiteturas funcionais de I&C (Especificação das interfaces transversas):
   a) Declinação funcional e classificação dos sistemas de I&C;
   b) Interfaces Funcionais e Condições da Planta; e
   c) Arquitetura funcional - Global de I&C.
3) Arquiteturas típicas de I&C (Especificação dos dados de entrada):
   a) Especificação das malhas de I&C;
   b) Catalogação das arquiteturas típicas;
   c) Alocação das malhas de I&C; e
   d) Geração de relatórios de entrada e saída, e de funções de controle.
4) Especificação de sistemas de controle:
   a) Descrição do Sistema de Controle;
   b) Caracterização do Sistema de Controle; e
   c) Operação do Sistema de Controle.

Os itens a seguir definem os atores, as entradas e a mínima informação que conteria em cada item de especificação.

3.4.4 Critérios gerais de I&C (Especificação de requisitos transversos)

A base que norteia os critérios gerais de I&C de qualquer empreendimento deve ser estabelecida pelos princípios de alto nível do projeto (nível 1 – UNM). Estes critérios gerais irão compor os Objetivos Gerais de Segurança e de Operabilidade, que permearão toda a análise funcional e estabelecimento de requisitos nos níveis subsequentes.

Como o propósito central desta seção é apresentar os critérios transversos que servem como balizadores para a especificação de sistemas e componentes relacionados com I&C, devem-se conhecer três conceitos fundamentais: visão funcional I&C, classificação de segurança das funções I&C, e as condições ambientais.

Os sistemas de I&C servem fundamentalmente para sentir o processo, enviar as variáveis medidas para que sejam controladas (automaticamente ou manualmente), para que sejam informadas (se necessário) aos operadores através das estações de trabalho e/ou painéis, para que os operadores tenham meios de atuar a planta manualmente (onde necessário), e para que os atuadores manipulem a variável de processo a partir de comandos dos controladores (automaticamente) ou dos operadores (manualmente) (INTERNATIONAL ATOMIC ENERGY AGENCY, 1999).

Visto isto, a classificação das funções é usualmente realizada usando a combinação de métodos determinísticos e de práticas e lições aprendidas de engenharia, levando em consideração: a função de segurança a ser executada (ações que respondem a alguns eventos AOO ou acidentais, ou que a falha pode causar um evento perigoso); a falha de uma função e suas consequências à segurança; o tempo de resposta de cada função e em quanto tempo será executada sem gerar um evento perigoso; e, a linha de ação e dependência de ações alternativas em relação à estratégia de DiD - NUREG/CR-6303 e NUREG/CR-7007 (NUCLEAR REGULATORY COMMISSION, 1994; NUCLEAR REGULATORY COMMISSION, 2009).

As funções de I&C serão classificadas (assim como componentes e equipamentos) a partir de classificações de funções dos níveis superiores. Neste trabalho, a exemplificação da metodologia se dará em conformidade com a norma ANSI/ANS-58.14. Devido às variações ambientais decorrentes das consequências acidentais, este trabalho recomenda que dentro da classificação geral, seja identificado se o item deverá suportar condições de acidente do tipo LOCA ("*Loss of Coolant Accident*") ou que não é LOCA.

Em linhas gerais, este item visa estabelecer em alto nível, de forma transversa, os critérios mínimos de I&C da UNM. Com isso, é possível definir a sequência de atividades e entregáveis por ator.

3.4.4.1 Delimitação do escopo dos Sistemas de I&C

Para a delimitação do escopo dos Sistemas de I&C, este trabalho constituiu os princípios gerais tomando como base a norma regulamentadora americana: 10CFR50 (Appendix A – General Design Criteria – GDC), que provê critérios gerais para os SSCs Importantes para Segurança:

> *The principal design criteria establish the design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety, that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.* (10CFR50: Appendix A – General Design Criteria – GDC).

Os critérios apresentados nos GDCs são considerados de alto nível, e aplicam-se transversalmente para todos os níveis funcionais e de sistemas, em todo ciclo de vida da UNM, e em todas as condições da planta (Manutenção, testes, operação normal, AOO e acidentais). Além disso, o próprio órgão regulador americano enfatiza que os GDCs não são suficientes para contemplar todas as peculiaridades de uma UNM, sendo necessário que em cada empreendimento seja realizada uma análise particular para adição de critérios com direcionamento para o interesse da segurança pública.

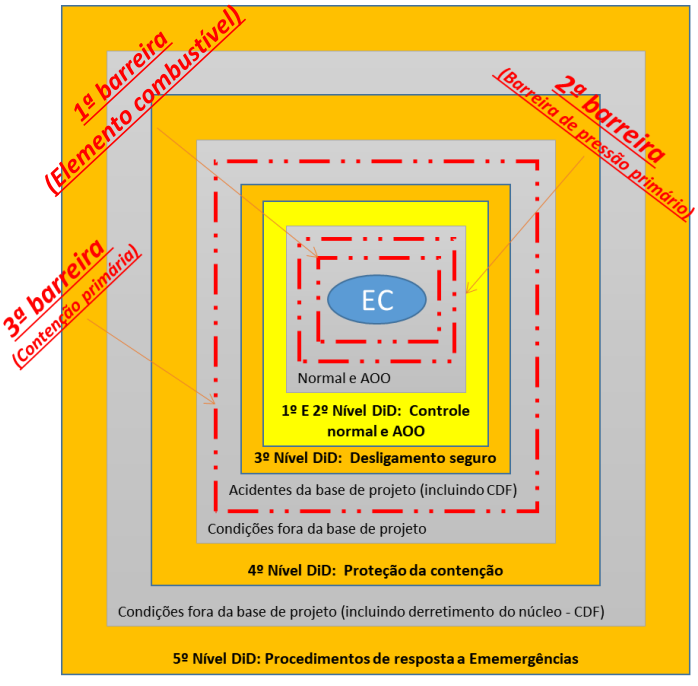
Em relação aos princípios nucleares do GDC, é possível constatar que eles levam em conta um conjunto de informações que contribuem tanto na elaboração da árvore funcional da UNM, quanto na especificação de requisitos funcionais. Ao longo do GDC é possível identificar:

- Estados da UNM (Normal, AOO, Acidental, LOCA, manutenção, teste e inspeção);
- Eventos da base de projeto (aumento da reatividade, exposição à radiação, perda de energia, travamento de barras, etc.);
- Funções de segurança (garantir que os limites de projeto do núcleo não sejam excedidos; ou, garantir que os limites de projeto da barreira de pressão do primário não seja excedido; ou, garantir que os limites de projeto da contenção não sejam excedidos; ou, garantir que o núcleo está sendo refrigerado, dentre outros); e,
- Sistemas (Sistema de Refrigeração do Reator; Sistema de Reposição de Refrigerante; Sistema de Proteção do Reator; Sistema Elétrico etc.).

Cruzando todas estas informações, constatou-se que o GDC é respaldado através da estratégica DiD. O conjunto dos requisitos e funções se distribui num arranjo concêntrico de barreiras de proteção e camadas de funções de segurança como meios de se atingir os objetivos de segurança nuclear. A consequência de se utilizar os princípios de DiD é que a UNM seja mais resiliente às falhas. Basicamente ele consiste em três camadas, ou escalões (*echelons*) de segurança: prevenção, proteção e mitigação (FRUTUOSO et al, 2011).

Na figura 14 são apresentadas as barreiras e níveis de defesa discriminados dentro do GDC, e adaptados para este trabalho com base nos trabalhos da WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION (2013) e refinados no guia da ELECTRIC POWER RESEARCH INSTITUTE (2014). Vale notar na figura os seguintes grupos: Estados da planta (Estado operacional – Normal & AOO; e Estado acidental – Base de projeto & Além da base de projeto), barreiras dos produtos de fissão (1ª barreira – Invólucro do elemento combustível; 2ª barreira – Barreira de pressão do primário; 3ª barreira – Contenção primária), e os níveis DiD (Nível 1, 2, 3, 4 e 5).

Figura 14 - Níveis de DiD, Barreiras de Proteção e Estados da UNM



A especificação dos requisitos relacionados com a segurança nuclear da UNM, deve portanto, ter como base estes princípios. A declinação destes princípios para os níveis inferiores precisam de revisão constante da equipe de análise de segurança na

perspectiva de garantir que as funções de segurança serão mantidas. Esta metodologia estabelece como requisito, que para a garantia da rastreabilidade, a taxonomia utilizada na identificação dos requisitos de segurança nuclear sejam estabelecidos de forma que haja uma origem (única) no nível 1. Que no nível 2 haja a alocação transversa dos GDCs a cada sistema que contenha função nuclear, e que nos níveis subsequentes os requisitos sejam declinados buscando critérios de normas complementares da base americana.

Ou seja, o nível 1 pode apresentar os requisitos do cliente e atendimento à base normativa (flexibilidade de atendimento zero). O nível 2 distribui os GDCs nas funções especificadas pelo nível 1 e 2. Já os níveis 3 e 4 aplicam as normas de projeto, como por exemplo as normas ANSI/ANS 51.1 e ANSI/ANS 58.14. Esta hierarquização de declinação dos requisitos nucleares constitui uma estruturação que atesta que a UNM pode ser operada sem pôr em risco a saúde e segurança dos trabalhadores, público e meio ambiente, por estar aderente à base normativa.

Após a constituição dos princípios gerais de segurança nuclear, é necessário apresentar as funções que são importantes para a segurança nuclear, conjuntamente com sua classificação. O objetivo é cumprir os objetivos gerais da UNM, dos princípios nucleares e dos eventos iniciadores. Sendo assim, este trabalho tomou por base o método racional das normas ANSI/ANS 51.1 e ANSI/ANS 58.14.

A metodologia aplicada às FIS, que devem operar para cumprir os princípios de segurança nuclear, segue a estratégia de declinação de cima-para-baixo, em conformidade com a base normativa. A análise funcional proposta, versará em determinar aquelas FIS que deverão prover meios para evitar ou mitigar as consequências de acidentes postulados que podem causar risco para a saúde e segurança dos trabalhadores, público e meio ambiente.

As funções da UNM de forma geral são separadas naquelas que são Importantes para a Segurança Nuclear (FIS) e naquelas que NÃO são Importantes para Segurança Nuclear (Não-FIS). Como as FIS são correlacionadas às condições operacionais da UNM, isto implica também que as FIS tem correlação com os níveis de defesa em profundidade, o que implica que as FIS tem correlação também com ao menos um requisito de segurança nuclear, originado dos princípios de segurança nuclear. Por outro lado, as Não-FIS referem-se apenas para aquelas funções que não são importantes pra segurança nuclear.

A classificação de segurança nuclear é um meio de identificar SSCs quanto a sua significância frente aos riscos e objetivos de segurança nuclear definidos nos níveis superiores de especificação em conformidade com a base normativa do projeto. Contudo,

a classificação dos componentes depende fundamentalmente das funções de serviço providos ou requeridos do exterior.

Como pode ser visto na Tabela 4, a WORLD NUCLEAR ASSOCIATION (2015) empreendeu esforços no sentido de correlacionar as classificações utilizadas pelos diversos agentes (órgãos reguladores e associações nucleares) para facilitar as trocas de informações.

Analisando a tabela 4, vale ressaltar a desarmonizarão entre os organismos de regulação nuclear americano e europeu em relação às classificações e principalmente em relação ao termo "*safety-related*".

Portanto, a classificação de segurança nuclear implica necessariamente, num primeiro momento, na categorização funcional, e num segundo instante, na classificação dos SSCs. A categorização de segurança é assim um processo onde se identificam as FIS de uma UNM conforme sua criticidade. Já o processo de classificação de segurança é aquele que atesta a classe de um SSC de acordo com a mais alta categoria funcional estabelecida a um específico SSC.

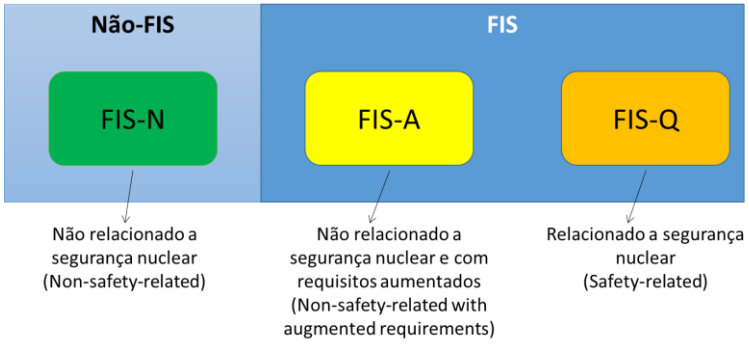
Tabela 4 - Correlação entre as diversas classificações de segurança

<table>
<tr><th colspan="2" rowspan="2">Organização</th><th colspan="4">Classificação de segurança de funções ou sistemas I&C em UNM</th></tr>
<tr><td rowspan="2">Items not important to safety</td><td colspan="3">Items importante to safety</td></tr>
<tr><td colspan="2" rowspan="2">U.S.NRC</td><td colspan="2">Non-safety-related</td><td>Safety-related</td></tr>
<tr><td>ANSI/ANS 51.1</td><td>SSC</td><td colspan="2">Non-safety-related (With and without special requirements)</td><td>Safety-related</td></tr>
<tr><td>ANSI/ANS 58.14</td><td>Funções e SSC</td><td>Non-safety-related [N]</td><td>Non-safety-related with augmented requirements [A]</td><td>Safety-related [Q]</td></tr>
<tr><td colspan="2" rowspan="2">IEEE</td><td rowspan="2">Non-safety-related</td><td colspan="2">Items importante to safety</td></tr>
<tr><td>(not specified)</td><td>Safety-related</td></tr>
<tr><td colspan="2" rowspan="3">IAEA Safety Glossary</td><td rowspan="4">Items not important to safety</td><td colspan="3">Items importante to safety</td></tr>
<tr><td colspan="2">Safety-related items</td><td rowspan="2">Safety systems</td></tr>
<tr><td>Safety features (for DEC)</td></tr>
<tr><td rowspan="2">IAEA SSG-30</td><td>Funções</td><td>Safety catefory 3</td><td>Safety category 2</td><td>Safety category 1</td></tr>
<tr><td>Sistemas</td><td>Safety class 3</td><td>Safety class 2</td><td>Safety class 1</td></tr>
<tr><td colspan="2" rowspan="3">IEC 61226</td><td rowspan="3">Systems not important to safety</td><td colspan="3">System Important to Safety</td></tr>
<tr><td>Funções I&C</td><td>Category C</td><td>Category B</td><td>Category A</td></tr>
<tr><td>Sistemas I&C</td><td>Class C</td><td>Class B</td><td>Class A</td></tr>
</table>

Fonte: adaptado de WORLD NUCLEAR ASSOCIATION (2015).

A classificação de um SSC serve para delimitar a aplicação de critérios de segurança nuclear no que se refere ao projeto, fabricação e qualificação. As aplicações destes critérios garantem assim a confiabilidade do SSC, garantindo que este estará apto a operar adequadamente quando requisitado para cumprir uma determinada função de segurança nuclear. Com estas definições, o trabalho propõe a classificação (ou categorização), código de cores e nomenclatura funcional conforme a figura 15.

Figura 15 - Visão geral da classificação funcional de segurança nuclear



Fonte: adaptado de ANSI/ANS 58.14

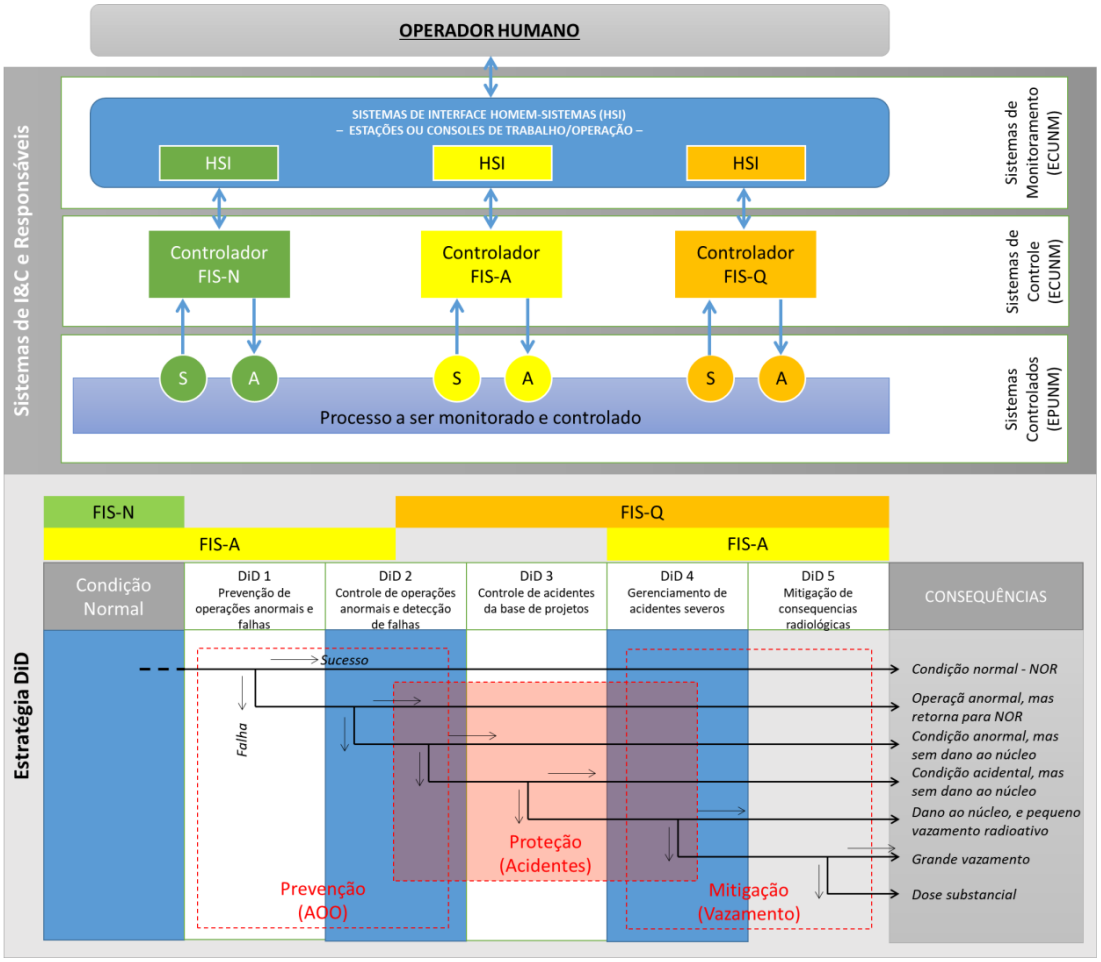
Com isso a análise funcional adotada neste trabalho tende a convergir com a estratégia de DiD, permitindo incorporar sistematicamente os conceitos de diversidade, programa de HFE e de segurança cibernética ("*cyber security*"). O conceito DiD permite estabelecer atributos (critérios de performance) para os muitos níveis de classificação dentro da análise funcional. Portanto, será realizada classificação de cada função a ser controlada a partir da análise de eventos iniciadores postulados, levando em consideração a consequência mais severa frente a frequência de ocorrência dos eventos. Neste interim, será possível incluir graus de liberdade ao projeto sem prejudicar os objetivos de segurança nuclear.

Com todo exposto, pode-se delimitar o escopo dos sistemas de I&C em níveis, como ilustrado na figura 16, onde constam os Sistemas Controlados ou simplesmente Processo (sensores e atuadores), e os Sistemas de Controle e Sistemas de Monitoramento ou simplesmente Supervisório, assim como os níveis DiD.

Cada um desses níveis deve ser classificado quanto à segurança nuclear, como: FIS-N (apenas em condições normais), FIS-A (em condições normais e transientes –

AOO) e FIS-Q (em condições transientes e acidentais), em conformidade com a base normativa americana proposta por este trabalho (para maiores detalhes ver o anexo 3).

Figura 16 - Macrovisão do escopo funcional



Fonte: adaptado de IAEA (2011) e EPRI (2014)

De acordo com a ANSI/ANS 58.14 as FIS-Q são funções importantes para a segurança nuclear que devem operar durante e após um evento da base de projeto para garantir as três funções básicas de segurança definidas pela 10CFR50: A integridade da barreira de pressão do refrigerante do reator (RCPB), ser capaz de desligar o reator (SCRAM), e os níveis máximos de vazamentos radioativos fora da UNM (*Potential off-site exposures*). Dentro do leque de funções de I&C classificadas como FIS-Q, teríamos aquelas envolvidas com: desligamento de emergência do reator (*Reactor trip*), resfriamento emergencial do núcleo, remoção de calor residual, isolamento da contenção,

remoção de produtos de fissão da contenção, remoção de calor da contenção, ventilação de emergência, e suprimento elétrico de emergência.

De acordo com a ANSI/ANS 58.14 as FIS-A são funções importantes para a segurança nuclear que devem operar em eventos especiais ou para atender requisitos advindos do órgão licenciador ou comitê de segurança. A 10CFR50.49 ressalta que algumas funções (tratadas como FIS-A neste trabalho) devem receber requisitos adicionais, pois suas falhas podem acarretar prejuízos às funções de segurança – "*Safety-related*" (FIS-Q), ou provêm certos monitoramentos pós-acidentais. Alguns exemplos de funções FIS-A seriam: controle de potência do reator, desligamento de emergência diverso do reator, controle do balanço massa e energia do primário (pressão, temperatura, vazão e inventário do elemento refrigerante), detecção de fogo, monitoramento da radiação, controles de acesso de pessoal, e monitoramento para plano de resposta emergencial.

Já as funções FIS-N seriam quaisquer outras funções que não são importantes para a segurança nuclear, requeridas apenas para as condições normais da UNM e irrelevantes para as outras condições (transientes e acidentes). Controle de alimentação de água para reaquecimento e controle da água desmineralizada são exemplos de funções para esta classificação. A tabela 10 do anexo 4 é um exemplo da aplicação desta especificação.

Este item visa a delimitação do escopo funcional dos sistemas de I&C, o que contribui com o processo decisório da estruturação funcional e sistêmica do AGUNM. Com isso, é possível contribuir na verificação do cumprimento dos requisitos, evitar o surgimento e/ou contribuir com soluções de conflitos entre o AGUNM (e equipe de controle a ele subordinada para esta atividade) e os projetistas dos sistemas de I&C (dos diversos níveis), e com as equipes de análise de segurança e licenciamento da UNM, motivando os atores e propondo os requisitos técnicos aplicáveis aos níveis 3.

3.4.4.2 Especificação dos meios disponíveis de operação

Esta especificação tem o propósito de definir os meios de operação da UNM, e deve cobrir os seguintes itens:

- Organização geral da operação da UNM:
  - Localização dos meios de operação;
  - Modos de operação em situações degradas;
- Os princípios de operação da UNM:

- Definição dos princípios de controle;
- Critérios para a especificação dos locais de controle.
- Critérios para a especificação dos níveis de automação.
- Critérios para a especificação de monitoramento e alarmes;
- Critérios para a especificação das operações de manutenção;
- Critérios para a especificação das interfaces humano-sistema.

O propósito geral destes princípios é garantir que todos os sistemas requeiram e especifiquem suas necessidades com a devida aderência aos meios disponíveis de controle da UNM (NUCLEAR REGULATORY COMMISSION, 2012). Caso contrário, poderão ocorrer demandas que não terão como ser atendidas, e que poderão causar retrabalhos para readequações. Outro benefício é o fato de que a ECUNM poderá receber demandas dos processos, não previstas nos princípios gerais, sendo assim descartadas. O que garante a rastreabilidade do projeto.

Para isso, estes itens mínimos poderão num primeiro instante fornecer de forma global, a quantidade de tripulantes que terão por atribuição controlar tanto os sistemas navais, quanto os sistemas nucleares. Nesta especificação é imperioso que sejam mencionados tanto as salas de controle disponíveis, e para a operação nuclear destacar quem serão os Operadores do Reator, se haverá supervisor, qual será a composição da equipe de proteção radiológica, e os técnicos que estarão envolvidos em ações corretivas e manutenção a bordo (incluindo os técnicos de automação e instrumentação).

É boa prática que na especificação sejam apresentados os consoles de operação disponíveis no projeto, com respectivas dimensões e localizações. Em situações degradadas devem ser descritos os outros modos de operação, principalmente no que se refere ao desligamento seguro do reator. Pode-se citar como exemplos, algumas situações degradadas relacionadas a uma planta nuclear embarcada: perda da sala de controle onde está o console de operação da planta nuclear, perda do console de operação da planta nuclear, perda do sistema de controle normal e perda do sistema de proteção da UNM.

Quanto aos princípios de operação, o primeiro passo é definir claramente a terminologia de controle e devidas abreviações. Devido ao elevado número de normas e organismos reguladores, podem ser originadas divergências tanto entre os atores dentro do empreendimento, quanto entre os fornecedores e validadores dos sistemas de controle (WORLD NUCLEAR ASSOCIATION, 2015). Alguns termos de controle estão listados no anexo 1 deste trabalho. Após o delineamento da terminologia utilizada, inicia-se a

especificação dos critérios de operação em si, definindo como se dará a seleção dos locais de operação pelas EPUNM.

Os critérios para seleção dos níveis de automação demandados pelo processo devem basear-se na frequência de atuação diária, no tempo requisitado para reação do operador, na carga de trabalho demandada pelo processo e na resposta do tempo de atuação. Como referência normativa da NRC, pode-se ter como referência a ANSI/ANS 58.8 (AMERICAN NATIONAL STANDARDS INSTITUTE. AMERICAN NUCLEAR SOCIETY, 2019). Esta norma detalha os critérios a serem considerados, levando-se em consideração as consequências dos acidentes nucleares. Como critério geral, as lógicas de proteção para os eventos de maior frequência destacados pela análise de segurança devem ser automáticos, mas isto não impede ações pelo operador.

Já no que se refere aos critérios de seleção do monitoramento e alarmes, deve-se ter em mente que nem todos os parâmetros do processo necessitam ser apresentados nas telas e painéis. Para isso, deve-se realizar um gerenciamento de alarmes que avalie o número de operações, ou seja, a carga de trabalho requerida pelo processo, quantificando os alarmes por minuto. Depois classificar estas demandas por critérios de aceitação, ou seja: não aceitável, alta demanda, gerenciável e aceitável. Dependendo da quantidade de alarmes demandados, o ponto ótimo é aquele onde os operadores sejam demandados somente com alarmes classificados como aceitáveis ou gerenciáveis, e alguns de alta demanda e críticos (NUCLEAR REGULATORY COMMISSION, 2012). Por último, esta especificação deverá contemplar os critérios gerais para propósitos de manutenção e ergonomia em relação às interfaces (NUCLEAR REGULATORY COMMISSION, 2020d).

A sumarização da aplicação desta especificação é demonstrada na tabela 11 do anexo 4, onde deve constar uma matriz com todos os meios de operação e suas respectivas classificações através de código de cores. Após a definição dos meios de operação, é gerado relatório com a lista dos meios de operação com respectivos subsistemas, equipe responsável, código de identificação, descrição e classificação funcional (Tabela 12).

Este item visa clarificar para todos os atores do projeto quais são os meios de operação da UNM, o que contribui com a elaboração das especificações operacionais dos diversos subsistemas. Com isso, é possível contribuir na verificação do cumprimento dos requisitos, evitar o surgimento e/ou contribuir com soluções de conflitos entre o AGUNM (e ECUNM a ele subordinada para esta atividade) e os projetistas dos sistemas de I&C

(dos diversos níveis), e com as equipes de análise de segurança e licenciamento da UNM, motivando os atores e propondo os requisitos técnicos aplicáveis aos níveis 3 e 4.

3.4.4.3 Plano Tecnológico de I&C

Esta especificação tem o propósito de definir o padrão de tecnologia de componentes de I&C a serem utilizados no projeto, e deve cobrir os seguintes campos (INTERNATIONAL ATOMIC ENERGY AGENCY, 1999 e 2011):

- Critérios para a especificação de sensores e atuadores;
- Critérios para a especificação de automação e redes;
- Critérios para a especificação de supervisórios e interfaces humano-sistemas; e,
- Critérios para a especificação de cabeamento.

Lembra-se também, que o plano tecnológico deve conter os seguintes requisitos:

- Condições ambientais: o projeto deve prever as condições de cada compartimento do navio, que contenham no mínimo informações relativas a: temperatura e umidade, pressão e composição da atmosfera, vibração, inclinações do navio, fadiga mecânica, parâmetros radiológicos, e outras forças ordinárias.
- Requisitos gerais de I&C: tolerâncias de faixas de operação, funcionalidade com ferramentas de calibração e ajustes, protocolos de comunicação, etc.
- Requisitos de suprimento de energia: níveis das fontes pneumáticas, hidráulicas ou elétricas.
- Requisitos de aterramento.
- Requisitos de proteção: quanto ao ambiente, quanto à vibração, quanto à interferências eletromagnéticas ou de radiofrequência, tropicalização, e de explosividade.
- Requisitos de materiais.
- Requisitos de instalação e arranjo: quanto à visibilidade, acessibilidade, minimização de efeitos vibratórios, ou fontes quentes, posição de instalação, etc.
- Requisitos de inspeção e testes.

Para organizar os requisitos, será utilizada a proposição de classificação de segurança conforme segue. Esta classificação servirá para melhor alocação das funções e correspondência aos sistemas da usina nuclear móvel.

- *Safety-related* [FIS-Q]:
    - Tipo Q (loca)
    - Tipo Q (non-loca)
- *Non-Safety-related with Augmented Requirements* [FIS-A]:
    - Tipo A (loca)
    - Tipo A (non-loca)
- *Non-Safety-related* [FIS-N]:
    - Tipo N

As tabelas 13, 14 e 15 do anexo 4 são exemplos desta especificação. Este item visa padronizar a tecnologia a ser adotada no projeto da UNM, o que contribui com a elaboração das especificações dos equipamentos e componentes dos diversos subsistemas, buscando a viabilidade do projeto frente ao processo de obtenção. Com isso, é possível contribuir na verificação do cumprimento dos requisitos, evitar o surgimento e/ou contribuir com soluções de conflitos entre as equipes de obtenção e os projetistas dos sistemas de I&C (dos diversos níveis), e com as equipes de análise de segurança e licenciamento da UNM, motivando os atores e propondo os requisitos técnicos aplicáveis ao nível 5.

3.4.5 Arquiteturas funcionais de I&C (Especificação de interfaces transversas)

Outro grupo de atividades a serem empreendidas pela ECUNM é especificar globalmente as interfaces transversas. Esta atividade visa evitar o surgimento de conflitos entre os atores do projeto, e facilitaria a solução de potenciais conflitos. Outra contribuição desta atividade é definir quais os requisitos técnicos seriam aplicáveis aos agentes destas especificações.

Para ajudar nestas especificações, este trabalho propõe a utilização dos conceitos de DiD. Isto se faz necessário, pois historicamente o conceito DiD tem sido uma das mais importantes estratégias para se garantir a segurança nas plantas nucleares e pode ser o caminho para identificar claramente as atividades para cada ator dentro dos conceitos de operação da UNM, sendo uma forma de evitar o surgimento de conflitos entre os atores

dentro do projeto, e facilitador nas análises de segurança e redução de riscos, principalmente no que se refere às falhas de modo comum (NUCLEAR REGULATORY COMMISSION, 1994).

A antecipação na redução de riscos dentro do projeto básico contribui para a maturidade do projeto. As linhas de defesa para a redução dos riscos propostos pela Areva no projeto da U.S. EPR (AREVA, 2007) , por exemplo, contêm dispositivos distribuídos em quatro linhas de defesa nos moldes da NUREG-6303, conforme pode ser visto na Tabela 5.

Tabela 5 - Conceituação das linhas de defesa pela U.S. EPR

NUREG/CR-6303 (linhas de defesa)	**Linhas de defesa - U.S. EPR**		
	Preventiva	**Principal**	**Redução de Riscos**
Controle normal	x	-	-
Trip do reator (RT)	-	x	-
Sistemas de segurança (ESF)	-	x	-
Monitoramento	x	x	x

Fonte: adaptado de AREVA, 2007.

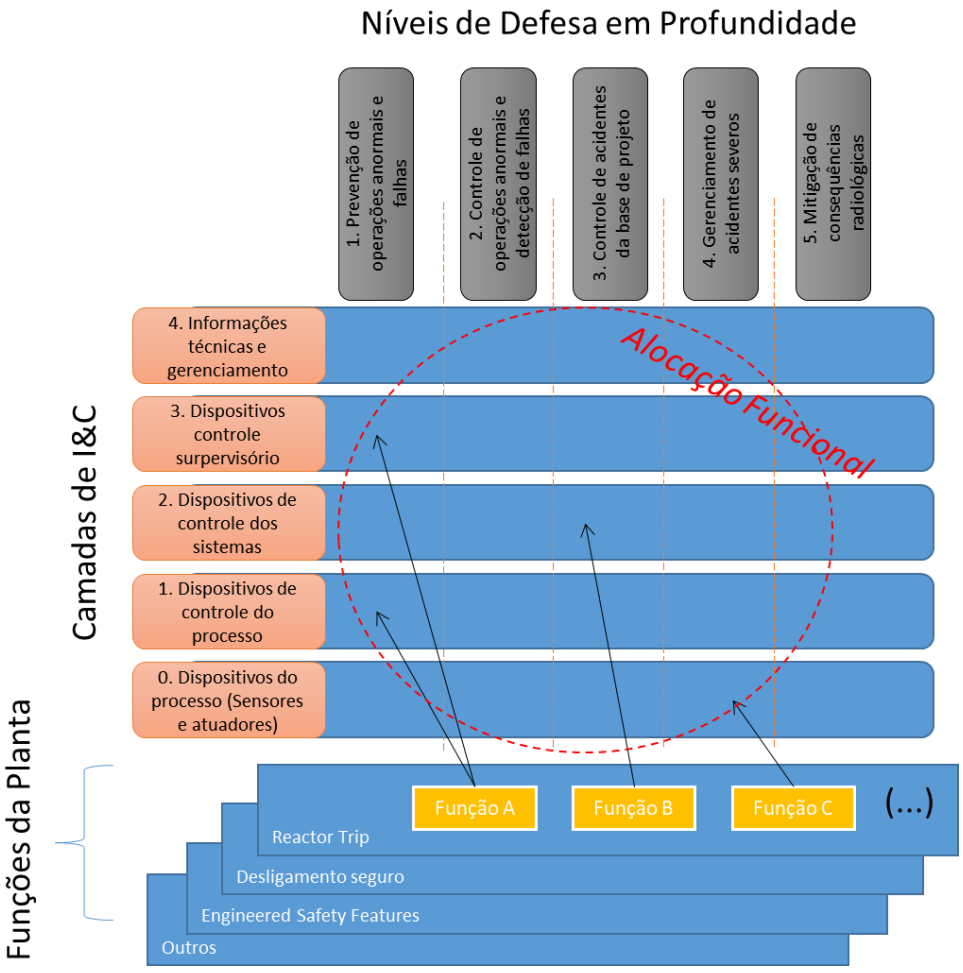
As linhas de defesa de mitigação de riscos se propõem a minimizar as consequências de eventos da base de projeto (por exemplo, ATWS e SBO), eventos sequenciados identificados pela análise probabilística de segurança (APS), experiências operacionais anteriores (por exemplo perda completa da realimentação de água principal e da realimentação de água de emergência), e ainda eventos de CCF e CMF de sistemas de segurança digitalizados, em conformidade com a BTP 7-19 da NUREG-0800 (NUCLEAR REGULATORY COMMISSION, 2021).

Nota-se que a transparência gerada por uma arquitetura DiD evitaria perdas de tempo, e outros riscos característicos quando não se há facilitação da troca de informações entre os diversos entes no projeto. A alocação de funções dentro de uma matriz de camadas de I&C "*versus*" níveis de defesa, levando-se em consideração os eventos ou cenários de operação dos diversos sistemas, dá condições (e motivações) para que todos os atores cooperem de forma contínua na implementação e melhoria da filosofia de operação da UNM.

Cabe salientar, que os atores responsáveis pelas funções de controle não podem, nem devem ser a ECUNM. Estas funções devem ser imputadas pelos líderes dos sistemas de processo (EPUNM). Todas estas funções não devem constar apenas das especificações com os conceitos de operação, mas, sobretudo devem considerar todas as situações complexas que acarretam os múltiplos eventos de falha, esclarecendo o nível do DiD específico àquela função de controle.

Com tudo isso, e ainda, a partir das definições dos níveis de defesa propostos para cada função de controle, composto inclusive de uma série de informações relevantes para se chegar a uma confiabilidade requerida, dar-se-á suporte para se definir detalhadamente as arquiteturas de I&C adequadas a cada situação. A figura 17 apresenta a conceituação proposta por este trabalho, seguindo o guia para desenvolvimento de arquiteturas de I&C - NP-T-2.11 (INTERNATIONAL ATOMIC ENERGY AGENCY, 2018).

Figura 17 - Alocação funcional na Arquitetura DiD



Fonte: adaptado de IAEA (2018).

A metodologia busca essencialmente consolidar todos os conceitos descritos de forma prática, orientada e transparente para que se obtenha uma redução da quantidade de trabalho ao longo do ciclo de vida do projeto. Isso obviamente, só poderá ser alcançado com base no fato de que todos os "*link*s" de informações estarão materializados de forma eficiente aos fluxos das informações. Os interessados não perderão mais tempo buscando-as, ou verificando se de fato aquela informação é a válida e liberada para uso no projeto.

A metodologia proposta contribui para o fluxo de informações buscando as quatro propriedades com foco na redução do tempo de trabalho ou custo global do projeto (FREIRE et al., 2018):

- Estabilidade: reter o procedimento ao longo do tempo;
- Robustez: manter o funcionamento face as perturbações;
- Resposta temporal: deve ser rápido;
- Previsibilidade: o processo deve ser uniforme, permitindo uma estimativa de custo precisa e melhorias contínuas.

Portanto, esta seção visa o estabelecimento da arquitetura geral de I&C (funcional). O que contribui em estabelecer a estratégia de declinação funcional e determinação de interfaces de I&C estabelecidas pelo AGUNM. Com isso, é possível contribuir na verificação do cumprimento dos requisitos, evitar o surgimento e/ou contribuir com soluções de conflitos entre o AGUNM (e ECUNM a ele subordinada para esta atividade) e os projetistas dos sistemas de I&C (dos diversos níveis), e com as equipes de análise de segurança e licenciamento da UNM, motivando os atores e propondo os requisitos técnicos aplicáveis aos níveis 3, 4 e 5.

O resultado deste item é a proposição gradual de arquiteturas funcionais, buscando a arquitetura geral de automação. O método para elaboração dos diagramas que compõem cada uma destas fases é descrito nos itens a seguir.

3.4.5.1 Declinação funcional e classificação dos sistemas de I&C

No primeiro passo para se obter a arquitetura geral de automação, trataremos de como dispor as classes de segurança nuclear da esquerda para a direita de acordo com sua significância à segurança nuclear: FIS-N (verde), FIS-A (amarelo) e FIS-Q (laranja). Esta disposição da classificação (da esquerda para a direita) permite correlação com os níveis de DiD, assim como com outras normas internacionais.

A utilização do código de cores busca evidenciar a classificação nas arquiteturas. Dispomos abaixo das classes, as funções de nível 3, para realizar uma demarcação matricial: sistemas/funções nível 4 versus classe/funções nível 3. Uma vez identificada a função e sistema, e alocada devidamente dentro da classificação e função nível 3, desmembramos a função nível 4 em funções técnicas.

O modelo para declinação funcional de alto nível está apresentado na tabela 16, e respectiva declinação funcional para o nível 4 na tabela 17 do anexo 4. Para compor o modelo os passos devem ser os seguintes:

a) Identificar que norma será utilizada para realizar a classificação funcional. As classificações deverão ser dispostas na parte superior do diagrama horizontalmente, da esquerda para a direita, da menos crítica para a mais crítica, facilitando a interação com as equipes de análise de segurança e licenciamento da UNM.
b) Identificar correlações normativas (Tabela 4) para facilitar a identificação e interações com fornecedores, e facilitando a interação com as equipes de obtenção da UNM.
c) Categorizar as diversas funções (FIS-Q, FIS-A e FIS-N) em grupos funcionais (nível 3) para permitir a declinação das funções técnicas para os níveis subsequentes (níveis 4 e 5), especificando as respectivas classificações de segurança e sistemas responsáveis.
d) Definir os blocos de funções técnicas de controle necessários para contemplar as necessidades das camadas de automação (sensores, atuadores, módulo ES, aquisição e condicionamento de dados, controlador, interfaces humano-sistema - HSI etc.).

Estes passos visam a devida alocação funcional, em suas respectivas classificações de segurança. Com isso, é possível definir a sequência de atividades e entregáveis por ator, contribuir na verificação do cumprimento dos requisitos, evitar o surgimento e/ou contribuir com soluções de conflitos entre os projetistas dos sistemas de I&C (dos diversos níveis) e as equipes de análise de segurança e licenciamento da UNM, motivando os atores e propondo os requisitos técnicos aplicáveis nos níveis 4 e 5.

O resultado deste item é apresentado na tabela 19 do anexo 4, tendo como referência para as funções técnicas a tabela 18.

3.4.5.2 Interfaces Funcionais e Condições da Planta

No segundo passo para se obter a arquitetura geral de automação, trataremos de dispor os sistemas, suas funções técnicas e interfaces dentro dos níveis DiD, em formato matricial. O eixo “x” caracteriza os níveis DiD, e o eixo “y” as camadas de automação.

O modelo para elaboração do diagrama DiD está na tabela 20 do anexo 4, tendo como resultado as interfaces da tabela 21. Para compor o diagrama os passos devem ser os seguintes:

a) Identificar horizontalmente (eixo x) a classificação de segurança (Q, A, ou N), em conjunto com os níveis de DiD: Nível 1 (operação normal), Nível 2 (Operação limitante), Nível 3 (Proteção contra acidentes), Nível 4 (Mitigação e proteção contra acidentes severos), e Nível 5 (Monitoramento de vazamento radioativo). Adaptado de INTERNATIONAL ATOMIC ENERGY AGENCY (2016).
b) Identificar verticalmente (eixo y) as camadas de automação: Camada 0 (nível de sensores e atuadores do processo), Camada 1 (nível de aquisição e envio de dados entre os sistemas de controle e o processo), Camada 2 (Controlador), Camada 3 (supervisório ou meios de operação). Adaptado de INTERNATIONAL ATOMIC ENERGY AGENCY (2018).
c) Alocar os diversos blocos funcionais dentro da matriz correspondente, demarcando os níveis DiD e camadas de automação aplicáveis.
d) Estabelecer as interfaces entre os diversos blocos funcionais, identificando a interface com a letra da classificação correspondente, seguindo o requisito da SSR-2/1 (INTERNATIONAL ATOMIC ENERGY AGENCY, 2012), em que a arquitetura deve ser tal que os níveis DiD sejam “*independent as far as practible*”.
e) Identificar as interfaces entre os diversos blocos funcionais, sequenciando/incrementando o mesmo identificador das arquiteturas DiD (por exemplo: N#1, N#2, A#1, A#2, A#3 etc.)

Este item visa especificar as condições operacionais, a função técnica equivalente à automação e respectivas necessidades de interfaces no projeto da UNM, o que contribui com a elaboração das arquiteturas de controle dos diversos subsistemas da UNM. Com isso, é possível contribuir na verificação do cumprimento dos requisitos, evitar o surgimento e/ou contribuir com soluções de conflitos entre os projetistas dos sistemas de

I&C (dos diversos níveis), motivando os atores e propondo os requisitos técnicos aplicáveis às arquiteturas de nível 3 e 4.

3.4.5.3 Arquitetura funcional – Global de I&C

No terceiro e último passo para se obter a arquitetura geral de automação, trataremos de dispor os blocos funcionais de forma que se estabeleça o declínio de cima para baixo, dos critérios propostos em alto nível pelo AGUNM. Esta arquitetura já se aproxima do perfil físico dos sistemas, o que permite uma padronização no modo de conceituação física das arquiteturas no nível 4 pelos ECUNM e EPUNM.

O modelo para elaboração da arquitetura geral de I&C é apresentado na figura 22 do anexo 4. Para compor o diagrama os passos devem ser os seguintes:

a) Dispor horizontalmente (eixo x) da esquerda para a direita os blocos de função (do menos crítico ao mais crítico – N, A e Q), buscando detalhar a conceituação da arquitetura DiD.
b) Identificar verticalmente (eixo y) os blocos de função nas camadas de automação na mesma terminologia utilizada na arquitetura DiD.
c) Detalhar a estratégia das interfaces de dados, especificando aquelas que devem ser por rede, fio (*hardwired*), ponto a ponto, e inserindo necessidades da base normativa, como segregações e isolamento.
d) Identificar as interfaces entre os diversos blocos funcionais, sequenciando/incrementando o mesmo identificador das arquiteturas DiD (por exemplo: se na DiD = A#1, então na Geral = A#1.1 e/ou A#1.2 etc.)

Este item visa dar as condições para detalhar as arquiteturas físicas no nível 4 do projeto da UNM. Com isso, é possível contribuir na verificação do cumprimento dos requisitos de baixo para cima, evitar o surgimento e/ou contribuir com soluções de conflitos entre os projetistas dos sistemas de I&C (dos diversos níveis), motivando os atores e propondo os requisitos técnicos aplicáveis às arquiteturas de nível 4.

3.4.6 Arquiteturas típicas de I&C (Especificação dos dados de entrada):

Esta seção visa dar os subsídios no nível 4, para que as EPNUM e ECUNM especifiquem seus sistemas na mesma filosofia estabelecida pelos critérios gerais de I&C trabalhadas nas arquiteturas funcionais. As arquiteturas típicas definirão as especificações

ou dados de entrada para as especificações tanto dos sistemas de processo, quanto para os sistemas de controle.

Estas arquiteturas estabelecerão de forma típica, os meios de controle e monitoramento de todas as variáveis e atuadores de processo. Sendo assim, ao projetista de processo caberá fornecer os subsídios mínimos para as arquiteturas típicas, através da especificações das malhas de controle mínimas necessárias para se estabelecer o controle do seu sistema. A ECUNM compilará estas necessidades, e especificará um catálogo de arquiteturas que poderão ser utilizadas pelas EPUNMs.

Através do catálogo de arquiteturas típicas, as EPUNMs selecionarão aquelas que atendem às suas demandas, o que chamamos neste trabalho de alocação das malhas de I&C. Após a alocação destas malhas de I&C, a ECUNM irá definir as interfaces físicas, gerando assim o relatório de entradas e saídas (ES) e de funções de controle (FC) para um pré-dimensionamento dos equipamentos de controle.

O resultado deste item é o escalonamento gradual de especificações no nível 4 do projeto, buscando a padronização dos meios de controle em arquiteturas típicas. Com isso, é possível contribuir na verificação do cumprimento dos requisitos de baixo para cima, evitar o surgimento e/ou contribuir com soluções de conflitos entre as ECUNM e EPUNM no nível 4, garantindo aderência com as equipes de análise de segurança e licenciamento da UNM, motivando os atores e propondo os requisitos técnicos aplicáveis aos níveis 4 e 5.

Os métodos para elaboração dos diagramas que compõem cada uma destas fases são descritas nos itens a seguir.

3.4.6.1 Especificação das malhas de I&C

A especificação das malhas de I&C deve dar-se pelas EPUNMs. O método para se chegar a esta especificação devem ser tais que seja possível estabelecer um diagrama de estados dos sistemas de processo. Neste diagrama de estados deve ser possível relacionar as configurações dos atuadores e/ou sensores de forma a caracterizar o modo de operação da planta.

Não é propósito deste trabalho detalhar esta especificação em todos os passos de concepção de um sistema de processo. O detalhamento da concepção da máquina de estados e as devidas configurações podem ser verificados no trabalho desenvolvido por

FREIRE (2018). Contudo este trabalho busca estabelecer passos fundamentais para cruzar as demandas de processo frente aos meios de controle disponíveis.

A especificação das malhas de I&C é uma atividade do processo, que deve conjuntamente estabelecer as suas necessidades de controle. Para isso, a EPUNM deve elencar as necessidades mínimas de controle para cada estado do seu sistema, e para cada fase (ou transição) entre os estados.

Os modelos para especificação das malhas de I&C estão nas tabelas 22 e 23 do anexo 4. Para a especificação das malhas, os passos devem ser os seguintes:

a) Definir as necessidades de controle e monitoramento dos sistemas para cada mudança de fase. De forma prática, deveriam ser listadas todas as transições, informado os estados de origem e destino, e depois especificar as necessidades, destacando aquelas que são remotas e locais. Este passo visa uma análise preliminar para a especificação do controle e monitoramento do processo.
b) Especificação do controle e monitoramento, utilizando os meios de controle disponíveis especificados pelos critérios gerais do projeto. Neste passo é fundamental listar todas as transições e estados, e para cada um detalhar aquelas necessidades de controle e monitoramento definidas no passo anterior. Assim que listar os estados e transições, definir as funções de controle, atuadores e/ou sensores, os parâmetros ou eventos associados, e a ação de controle a ser tomada. Depois deverão ser identificados quais dos meios disponíveis serão os responsáveis por executar o controle ou monitoramento.

Este item visa dar as condições de se especificar as funções de controle no nível 4 do projeto da UNM. Com isso, é possível evitar o surgimento e/ou contribuir com soluções de conflitos entre os projetistas dos sistemas de I&C (dos diversos níveis), motivando os atores e propondo os requisitos técnicos aplicáveis às arquiteturas de nível 4.

3.4.6.2 Catalogação das arquiteturas típicas

A especificação das arquiteturas típicas de I&C deve ser realizada pela ECUNM. O método para se chegar a esta especificação deve ser tal que garanta a padronização dos meios de controle e monitoramento com as demandas dos outros sistemas a serem

controlados. Estas arquiteturas deverão contemplar também os critérios gerais estabelecidos pelo AGUNM, no que tange escopo, classificação e tecnologias de I&C.

A elaboração das arquiteturas típicas de I&C é uma atividade do controle. Para isso, o projetista do sistema de controle deve explodir as interfaces funcionais estabelecidas na arquitetura geral, e apontar já para as categorias dos equipamentos físicos definidos pela ECUNM, ou para as categorias de equipamentos.

Nas figuras 23 e 24 do anexo 4 são apresentados modelos de arquiteturas típicas. As tabelas 24 e 25 apresentam as especificação de cada interface de dados das arquiteturas típicas. Para a elaboração das arquiteturas típicas, os passos devem ser os seguintes:

a) Já ter definido quais são os equipamentos que efetuarão o controle e monitoramento da UNM. Neste passo a ECUNM já deve possuir o diagrama básico da sua arquitetura.
b) Estabelecer arquiteturas típicas para cada escopo do controle, com os respectivos equipamentos e por tipos de atuadores e variáveis do processo. Sugere-se que se tenha um código identificador para cada típico, por exemplo: N_F1 (Medição de vazão executada via um sistema de controle não importante para a segurança nuclear).
c) No diagrama, cada componente de I&C deverá estar disposto nas camadas de automação (conforme arquitetura geral), e as interfaces de dados devem estar identificadas de forma a permitir a rastreabilidade definida em passos anteriores (por exemplo: se DiD = A#1, e na Geral = A#1.1, então no típico A#1.2.1 e/ou A#1.2.2 etc.)
d) Cada arquitetura típica deverá especificar o sinal, quantidades de sinais e tipo de sinal para todas as interfaces. Este passo permitirá a retirada de relatórios de entrada e saída de sinais de cada componente de I&C.

Este item visa dar as condições de se especificar as funções de controle no nível 4 do projeto da UNM. Com isso, é possível evitar o surgimento e/ou contribuir com soluções de conflitos entre os projetistas dos sistemas de I&C (dos diversos níveis), motivando os atores e propondo os requisitos técnicos aplicáveis às arquiteturas de nível 4.

3.4.6.3 Alocação das malhas de I&C

A alocação das malhas de I&C deve ser feita pela EPUNM em conjunto com a ECUNM. O método para se alocar as malhas pode ser via um sistema de engenharia ou um procedimento documental. Contudo, devido ao potencial computacional em estabelecer um banco de dados relacional, este seria o caminho mais eficaz neste passo.

A alocação das malhas de I&C é uma atividade da EPUNM, verificada pela ECUNM, e que devido aos passos anteriores garantirá o entregável específico, ou seja, os relatórios de entrada e saída e de funções de controle. Para isso, a EPUNM deve avaliar as malhas de controle necessárias pelo processo, e relacionar cada uma delas a uma arquitetura típica específica.

Os modelos para a alocação das malhas de I&C estão nas tabelas 26 e 27 do anexo 4. Para a alocação das malhas, os passos devem ser os seguintes:

a) A EPUNM deve selecionar cada malha de I&C individualmente, e direcionar a uma arquitetura típica.
b) A ECUNM deve verificar cada arquitetura (agora individualizada), verificar se já está alocado qual o equipamento que será o responsável por executar o controle, e em caso negativo (pois a arquitetura típica pode ter sido elaborada com equipamentos redundantes, por exemplo), especificar o equipamento responsável pelo controle daquela malha.

Este item visa dar as condições de se alocar arquiteturas às malhas de controle no nível 4 do projeto da UNM, para geração dos relatórios de entrada e saída e de funções de controle. Com isso, é possível evitar o surgimento e/ou contribuir com soluções de conflitos entre processo e controle no nível 4, motivando os atores e propondo os requisitos técnicos neste nível.

3.4.6.4 Geração de relatórios de Entrada e Saída e de funções de controle.

A geração de relatórios de entrada e saída (ES) e de funções de controle (FC) deve ser executada pela ECUNM, em conjunto com a EPUNM. O método para se gerar os relatórios pode ser via um sistema de engenharia ou um procedimento documental. Contudo, devido ao potencial computacional em estabelecer um banco de dados relacional, este seria o caminho mais eficaz neste passo.

A geração dos relatórios de ES e FC é uma atividade da ECUNM, verificada pela EPUNM, e que devido os passos anteriores garantirá o entregável específico, ou seja, os dados de ES e FC para dimensionamento dos equipamentos de controle.

O modelo do relatório de ES e FC está na tabela 28 do anexo 4. Para a geração do relatório de I&C, os passos devem ser os seguintes:

a) A ECUNM deve selecionar cada arquitetura específica gerada a partir da alocação das malhas de I&C, e levantar uma lista das interfaces de dados de cada uma delas, compilando-as numa única lista.
b) A lista do relatório deve contar no mínimo as seguintes informações: a identificação do sistema (nível 4), do equipamento a ser controlado ou sensor a ser monitorado, a descrição do controle, o código identificador do atuador/sensor, o tipo de sinal (digital ou analógico), a estratégia lógica (se positiva: 1 para atuar, ou se negativa: 0 para atuar), o detalhe do sinal (se 24Vcc, 4a20mA etc.), o range de controle e unidade de engenharia, o tipo de interface física (se direta ou indireta), a descrição e código identificador do equipamento de controle, e comentários gerais.
c) A EPUNM deve verificar a lista, certificando que as interfaces de controle atendem a todas as necessidades do processo.

Este item visa dar as condições de se levantar as demandas mínimas provenientes do processo, para especificação do sistema de controle da UNM. Com isso, é possível evitar o surgimento e/ou contribuir com soluções de conflitos entre processo e controle no nível 4, motivando os atores e propondo os requisitos técnicos neste nível.

3.4.7 Especificação de sistemas de controle

A especificação dos sistemas de controle é o objeto fim deste trabalho. Nesta especificação deverão constar os dados mínimos que demonstrem ao AGUNM, que os sistemas de controle contêm maturidade suficiente dentro do planejado.

Sendo assim, a especificação deverá dar condições para estabelecimento da "*design baseline*" que caracteriza os sistemas de controle, em nível de maturidade tal que permita o prosseguimento do projeto. Nesta especificação são dadas as configurações funcionais, os requisitos funcionais e não-funcionais, a arquitetura base, seus modos de operação e dados de entrada.

O resultado deste item é a sumarização das especificações e requisitos no nível 4 do projeto. Esta especificação contribui também com a verificação do cumprimento dos requisitos de baixo para cima, evitando o surgimento e/ou contribuindo com soluções de conflitos entre a ECUNM e EPUNM no nível 4, garantindo aderência com as especificações do AGUNM e com as equipes de análise de segurança e licenciamento da UNM, motivando os atores e propondo os requisitos técnicos aplicáveis aos níveis 5.

O método para elaboração da especificação dos sistemas de I&C foi particionar a especificação em três itens (descrição, caracterização e operação), apresentados a seguir. Os modelos de cada item são apresentados no anexo 4.

3.4.7.1 Descrição do Sistema de Controle

Na especificação dos sistemas de I&C deve ter um item dedicado a descrever em linhas gerais o sistema. Nesta descrição é importante que seja dada uma visão geral da estruturação sistêmica proposta do nível 1 ao nível 4, relacionando todos os sistemas pais do sistema de controle em questão (Tabela 29). Nesta descrição, podem ser indicados os principais equipamentos que estariam no nível 5, apontando para suas principais características e classificações de segurança e/ou disponibilidade.

Um primeiro subitem da descrição seria sobre as funções de serviço declinadas ao sistema de controle (Tabela 30). Uma boa forma de se descrever estas seções seria em tabela, contendo o código identificador da função (dos sistema de engenharia se for o caso), o código da função de segurança (normalmente elencadas pelas equipes de segurança nuclear), o nome da função, e a justificativa da função.

Um segundo subitem é a descrição das interfaces do sistema de controle. Neste item é imperativo que se tenha um diagrama que facilite a interpretação e verificação de cada interface e uma tabela que descreva as interfaces. As interfaces podem ser de grosso modo classificadas como funcionais (fluido ou dados) e físicas (alocação e arranjo). As interfaces funcionais seriam aquelas que de fato estabelecem o fluxo de informações entre os sistemas, no provimento do objetivo da UNM como um todo. Já as interfaces físicas seriam aquelas necessárias para a construção e montagem dos elementos fisicamente.

Ainda em relação ao subitem de interfaces, sugere-se que no diagrama sejam identificadas ambas as interfaces do sistema (requerida e provida). Outro ponto, é que no diagrama disponham de blocos que representem os sistemas e setas que representem as interfaces. Sugere-se que na interface requerida, por se tratar de um serviço solicitado

pelo sistema de controle, a seta saia do sistema que serve e chegue ao sistema de controle. No caso das interfaces providas, a seta sai do sistema de controle e vai para o sistema que está sendo controlado. Esta adoção caracteriza melhor o fluxo de informação resultante. O resultado do diagrama é uma tabela com a descrição das interfaces (Tabela 31).

Um terceiro subitem é a arquitetura física básica do sistema (Figura 25). Neste diagrama, é importante que sejam apresentados todos os equipamentos do sistema de controle, e que estes estejam dispostos de forma que se possa identificar a região onde o equipamento será alocado (não precisa haver detalhes). Este diagrama servirá de base para o arranjo definitivo dos equipamentos, e para avaliação com os times de segurança de qual agressão os equipamentos podem estar sujeitos ou causar, e às condições ambientais do local.

Um quarto subitem seria o arranjo dos equipamentos (Figura 26 e Tabela 32). Caso o projeto utilize uma maquete eletrônica, poderiam ser disponibilizadas fotos do arranjo destes equipamentos para facilitação do entendimento geral. Caso não haja recursos de maquete eletrônica, deverão conter neste item plantas baixas e em cortes que apresentem a localização dos equipamentos. Isto se faz fundamental para as análises de segurança e de encaminhamento de cabos preliminarmente. Alerta-se para o fato que as penetrações de cabos em unidades nucleares móveis podem ser críticas para fins de viabilidade do projeto.

O quinto e último subitem seria a lista dos equipamentos do sistema de controle (Tabela 33). Esta lista pode ser uma tabela que contemple no mínimo o código identificador do equipamento, sua designação, sua localização, sua criticidade e classificações (de segurança nuclear, de disponibilidade etc.).

3.4.7.2 Caracterização do Sistema de Controle

Na especificação dos sistemas de I&C outro item proposto por este trabalho é dedicado a caracterizar o sistema. Esta caracterização é fundamental, pois é a compilação de todas as especificações de alto nível, e que estabelecem o "*design baseline*" do sistema. Este é o principal item a ser entregue a todo o contexto do empreendimento.

Um primeiro subitem da caracterização é a funcional (Tabela 34). Neste subitem é dada uma descrição sucinta da principal função de serviço do sistema de controle, aquela que dá origem ao sistema em si, e que sem ela todas as outras funções e requisitos não teriam sentido. Aqui deve ser elencada o desempenho do sistema para que a função de

serviço seja atendida. Para isso, deve ser especificado o número de malhas de controle atendidas, com a respectivas demandas de entrada e saída de dados e funções de controle.

O relatório de requisitos para PLC comerciais da ELECTRIC POWER RESEARCH INSTITUTE (2009) pode ser utilizado para a especificação dos desempenhos. Alguns importantes desempenhos que devem ser especificadas são aquelas relativas às telas das estações de trabalho, de rede de dados, tempos de resposta de processamento e de aquisição e envio de dados etc. Tipicamente, os desempenhos seriam em relação à variação da tensão de entrada, do carregamento dos módulos de ES, processamento de dados nos controladores e fluxo de dados nas redes de controle.

Um segundo subitem é a caracterização dos equipamentos (Tabela 35). Para isso, deverão ser especificados os requisitos dimensionais (largura, profundidade, altura e espaços para acesso e manuseio do equipamento), de restrições referentes aos critérios de segurança e saúde dos trabalhadores, e de outros critérios gerais referente a I&C (conexões, modos de acesso etc.) e elétrica.

Um terceiro subitem é referente aos balanços gerais da UNM. Em um projeto dessa característica (espaço restrito) se faz necessário verificar constantemente pontos críticos que tornariam o projeto inviável. Portanto, neste tipo específico de projeto deverão ser realizados balanços de peso (Tabela 36), de necessidade suprimento de energia elétrica e de resfriamento do ambiente (Tabela 37), dentre outros. No caso de sistemas de controle, o projetista deve levantar as estimativas de peso, consumo elétrico e dissipação de calor para o ambiente. Estes dados necessitam ser qualificados, e avaliados quanto a sua maturidade para que os responsáveis pelo balanço global em cada área tenham condições de avaliar as linhas de tendência.

Um quarto e último subitem seria a dos requisitos não-funcionais, também chamados de restrições e requisitos transversos. Neste subitem, deverão estar os requisitos declinados para o sistema de controle, e as especificações de nível 4 e 5 que provem deles. Poderíamos citar que tais requisitos se referem a segurança não nuclear (Tabela 38), que contenha as condições ambientais, engenharia de fatores humanos (HFE) e segurança cibernética. Outros requisitos não funcionais que se referem à segurança nuclear (Tabela 39). Restrições de projeto (Tabela 40) em relação ao conforto (acústico, visual etc.) e compatibilidade eletromagnética. Requisitos de construtibilidade, manutenibilidade e logística (Tabela 41). E por fim, requisitos de normas de segurança para o trabalhador e qualidade (Tabela 42).

Este trabalho não tem por finalidade a especificação detalhada de cada item. Entretanto, poderíamos destacar as seguintes normas de referência que podem servir de parâmetro para a especificação dos requisitos não-funcionais: IEC 61513:2011 (*Instrumentation and control important to safety - General requirements for systems*); IEC 62340:2007 (*Requirements for coping with common cause failure*); IEEE P2425 (*Electromagnetic compatibility testing of electrical, instrumentation, and control equipment*); IEC 62003:2020 (*Requirements for electromagnetic compatibility testing*); Reg Guide 5.71 2010 (*Cyber security programs for nuclear power reactors*); IEC 62645:2019 (*Cyber security Requirements*); Reg Guide 1.152 Revision 3 (*Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*); IEC 62859:2016 (*Requirements for coordinating safety and cyber security*); IEC 60951-1:2009 (*Radiation monitoring for accident and post-accident conditions - Part 1: General requirements*); Reg Guide 1.152 2011 (*Use of computers in safety systems*); IEEE 7-4.3.2™-2016 (*Criteria for programmable digital devices in safety systems*); IEC 60987:2007 (*Hardware design requirements for computer based systems*); IEC 61500:2018 (*Data communication in systems*); Reg Guide 1.172 2013 (*Requirement specifications for software and complex electronics used in safety systems*); IEEE 830™-1998 (*Software requirements specifications*); Reg Guide 1.30 1972 (*Quality assurance requirements for the installation, Inspection, and testing of 1E power, instrumentation, and electrical equipment*); IEEE 336™-2010 (*Installation, inspection, and testing of 1E power, instrumentation and control equipment*).

3.4.7.3 Operação do Sistema de Controle

Na especificação dos sistemas de I&C, a última proposição se refere a descrição de operação dos sistemas. Para isso, é fundamental ter profundo conhecimento sobre as funções de serviço do sistema, e como foi realizada a declinação desde o mais alto nível. Este conhecimento será preponderante no momento de se definir o modo de operação dos sistemas frente as necessidades do AGUNM. Caso contrário, sua entrega será dissonante do contexto "*top-down*".

Um primeiro subitem seria a configuração funcional frente aos estados da UNM (tabelas 43 e 44). Cabe, portanto listar as funções dos sistemas, e estabelecer a condição de cada uma em relação à disponibilidade (disponível, indisponível, ou irrelevante). Essa visão, é importante para que sejam definidos os estados e transições do sistema.

Num segundo subitem é definido o diagrama de estados dos sistemas de controle. Seguindo o padrão de universo de estados em FREIRE (2018), foi possível pensar num diagrama de estados (Figura 27) intimamente ligado ao modo de operação, sendo quatro os estados assumidos: nominal (o sistema está operando na eficiência esperada), degradado (o sistema está operando fora da eficiência esperada ou não está operando, sendo uma redução de desempenho não intencional ou falha), desligado, e manutenção (que pode ser corretiva, preventiva ou até mesmo preditiva).

Ainda neste subitem, seria interessante realizar um pré-detalhamento das fases, relacionando-as com os domínios operacionais (normal, incidental ou acidental), com os modos de operação (partida, desligamento, degradado, manutenção etc.), com a disponibilidade funcional, com relação aos status (% do nominal, tipo de manutenção etc.), com os parâmetros para verificação da transição (início e fim) e com as principais alterações na configuração dos equipamentos/componentes.

Um terceiro subitem seria especificar as necessidades de controle e monitoramento do próprio sistema de controle (de forma similar ao realizado para os sistemas de processo – Tabelas 22 e 23), e definir os meios de controle e monitoramento dos sistemas de controle, para cada estado e transição.

4 RESULTADOS E DISCUSSÃO

Como resultado deste trabalho, temos o conjunto de modelos do anexo 4, que estabelecem uma metodologia de fluxo contínuo de projeto com vistas à especificação dos sistemas de I&C: especificando os critérios gerais de I&C (escopo, meios de operação e plano de tecnologia), depois estabelecendo as arquiteturas funcionais de I&C (definindo os blocos funcionais, as interfaces funcionais e a arquitetura geral), depois estabelecendo as arquiteturas típicas de I&C (definindo as malhas de I&C, catalogando as arquiteturas típicas, alocando as malhas às arquiteturas e gerando os relatórios de ES e FC), e por fim, especificando os sistemas de controle (descrição, caracterização e operação).

4.1 Atendimentos aos requisitos da Lei Construtal

Avaliando o resultado deste trabalho (modelos do anexo 4) frente aos requisitos da metodologia proposta por FREIRE (2018) – ver anexo 2, pudemos constatar que as atividades permitem o atendimento dos critérios de uma metodologia com vistas à lei construtal. Como apontado no trabalho, toda a metodologia se calçou principalmente nas hipóteses 2 e 3 de FREIRE (2018) – ver tabelas 2 e 3. Destas hipóteses de atendimento da Lei Construtal, para assegurar a passagem de fluxos, o canal precisa facilitar o escoamento, reduzir a contaminação e preservar a integridade da informação, assim como, deve maximizar o fluxo com menor custo esperado na curva total *versus* segurança.

Para justificar este entendimento, a linha metodológica proposta por este trabalho buscou responder às seguintes questões: qual a sequência das atividades por ator? Quais os requisitos de cada entregável? Como verificar o cumprimento dos requisitos? Como evitar o surgimento de conflitos entre atores? Como solucionar conflitos entre atores? Como motivar os atores? Quais os requisitos técnicos aplicáveis ao caso particular?

Na tabela 6 são apresentadas as respostas destas questões, destacando o sequenciamento das atividades numa estratégia de cima para baixo. É possível também notar a entrega de baixo para cima, da especificação proposta por este trabalho, o que visa a aplicação do modelo em V. Como descrito no trabalho, toda estratégia visa a declinação das especificações para os atores dos níveis inferiores, e uma posterior verificação e validação das especificações pelos atores de mais alto nível.

Tabela 6 - Respostas da linha metodológica à aplicabilidade da lei construtal

Sequência de atividades*			**Requisitos de projeto (Lei Construtal)**		**Conflitos entre atores**		**Requisitos Técnicos**
Cód.	**Ator (De)**	**Ator (Para)**	**Quais****	**Verificável**	**Evitado**	**Mitigação**	
1.a	AGUNM (N2)	EPUNM & ECUNM (N3)	Escopo funcional***	Sim	Sim	-	10CFR50 (App. A); NUREG-6303; ANSI/ANS 58.14
1.b	AGUNM (N2)	EPUNM & ECUNM (N3)	Meios de operação	Sim	Sim	-	NUREG-6303; ANSI/ANS 58.8; NUREG-0711
1.c	ECUNM (N2)	EPUNM & ECUNM (N3)	Plano tecnológico	Sim	Sim	-	ANSI/ANS 58.14; IAEA NP-T-3.12
2.a	AGUNM (N2)	EPUNM & ECUNM (N3)	Declinação funcional e classificação	Sim	Sim	-	ANSI/ANS 58.14
2.b	AGUNM (N2)	EPUNM & ECUNM (N3)	Interfaces funcionais e condições da planta	Sim	Sim	-	ANSI/ANS 51.1; ANSI/ANS 58.14; NUREG-6303
2.c	ECUNM (N3)	EPUNM & ECUNM (N4)	Arquitetura global e interfaces	Sim	Sim	Sim	IAEA NP-T-2.11
3.a	EPUNM (N4)	ECUNM (N4)	Malhas de controle	Sim	Sim	Sim	FREIRE (2018)
3.b	ECUNM (N4)	EPUNM (N4)	Arquitetura típica	Sim	Sim	Sim	IAEA NP-T-2.11
3.c	EPUNM (N4)	ECUNM (N4)	Alocação das malhas de controle	Sim	Sim	Sim	IAEA NP-T-2.11
3.d	ECUNM (N4)	ECUNM (N4)	Relatório ES e FC	Sim	Sim	Sim	IAEA NP-T-2.11
4.a	ECUNM (N4)	ECUNM (N3) & AGUNM (N2)	Descritivo sistema	Sim	Sim	Sim	NUREG-0800 (section 7)

Sequência de atividades*			Requisitos de projeto (Lei Construtal)		Conflitos entre atores		Requisitos Técnicos
Cód.	**Ator (De)**	**Ator (Para)**	**Quais****	**Verificável**	**Evitado**	**Mitigação**	
4.b	ECUNM (N4)	ECUNM (N3) & AGUNM (N2)	Caracterização do sistema	Sim	Sim	Sim	NPT-T-3.12
4.c	ECUNM (N4)	ECUNM (N3) & AGUNM (N2)	Operação do sistema	Sim	Sim	Sim	NUREG-0700 NUREG-6303

Obs.:
**Assumimos que todas as atividades, por terem atribuições e sequenciamento bem distribuído entre os atores de forma transparente, motiva a equipe.*
*** Cabe destacar que a descrição das atividades dentro do campo dos requisitos visa o mapeamento da aplicabilidade de tais requisitos. Os requisitos são apresentados em detalhe no Anexo 2 deste trabalho.*
**** A atividade do escopo funcional embora seja global, foi destacada no quadro, pois ela estabelece o "contrato" entre o arquiteto geral (quem declina as funções para cada sistema do nível inferior atribuindo o escopo de cada subsistema) e as ECUNM.*

4.2 Análise e discussão dos dados

O confronto realizado neste trabalho (anexo 2), resultou em uma relação N para N das atividades propostas por este estudo e os requisitos da tese de FREIRE (2018). Na tabela 7 é apresentada a distribuição dos requisitos da metodologia proposta por FREIRE (2018) nos grupos de atividades propostas por este estudo.

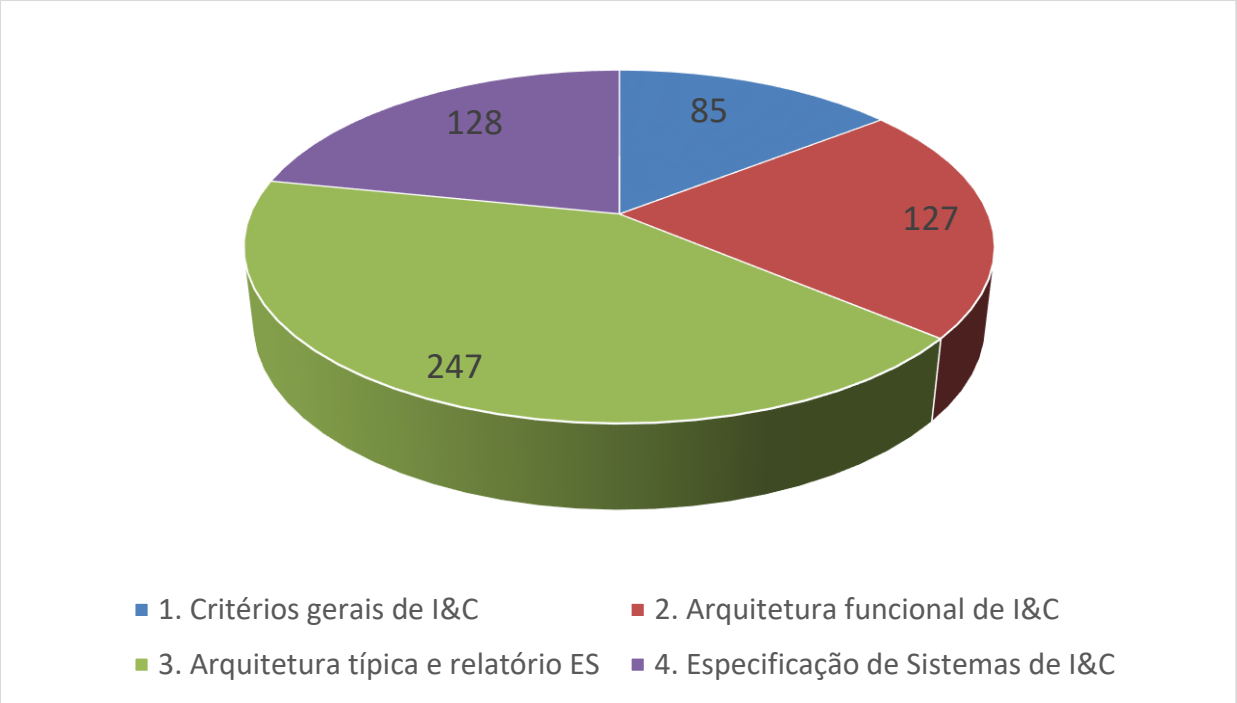
Tabela 7 - Requisitos da lei construtal na metodologia do trabalho

Atividades		Requisitos à luz da Lei Construtal				
		Total	**Desejável**	**Obrigatório**	**Negociável**	**Opcional**
1. Critérios gerais de I&C	1.a - Escopo funcional	8	3	4	1	0
	1.b - Meios de operação	28	6	13	6	3
	1.c - Meios de operação	49	19	19	8	3
2. Arquitetura funcional de I&C	2.a - Declinação funcional e classificação	21	9	11	1	0
	2.b - Interfaces funcionais e condições da planta	38	10	17	8	3
	2.c - Arquitetura global e interfaces	68	23	29	11	5
3. Arquitetura típica e relatório ES	3.a - Malhas de I&C	60	20	27	10	3
	3.b - Arquitetura típica	71	24	31	11	5
	3.c - Alocação das malhas de I&C	60	20	27	10	3
	3.d - Relatório ES e FC	56	19	24	10	3

Atividades		Requisitos à luz da Lei Construtal				
		Total	Desejável	Obrigatório	Negociável	Opcional
4. Especificação de Sistemas de I&C	4.a - Descritivo sistema	30	10	14	6	0
	4.b - Caracterização do sistema	47	18	17	9	3
	4.c - Operação do sistema	51	18	21	7	5

Na figura 18 é apresentada a distribuição gráfica do levantamento dos requisitos da tabela 7.

Figura 18 - Distribuição dos requisitos de projeto à luz da Lei Construtal

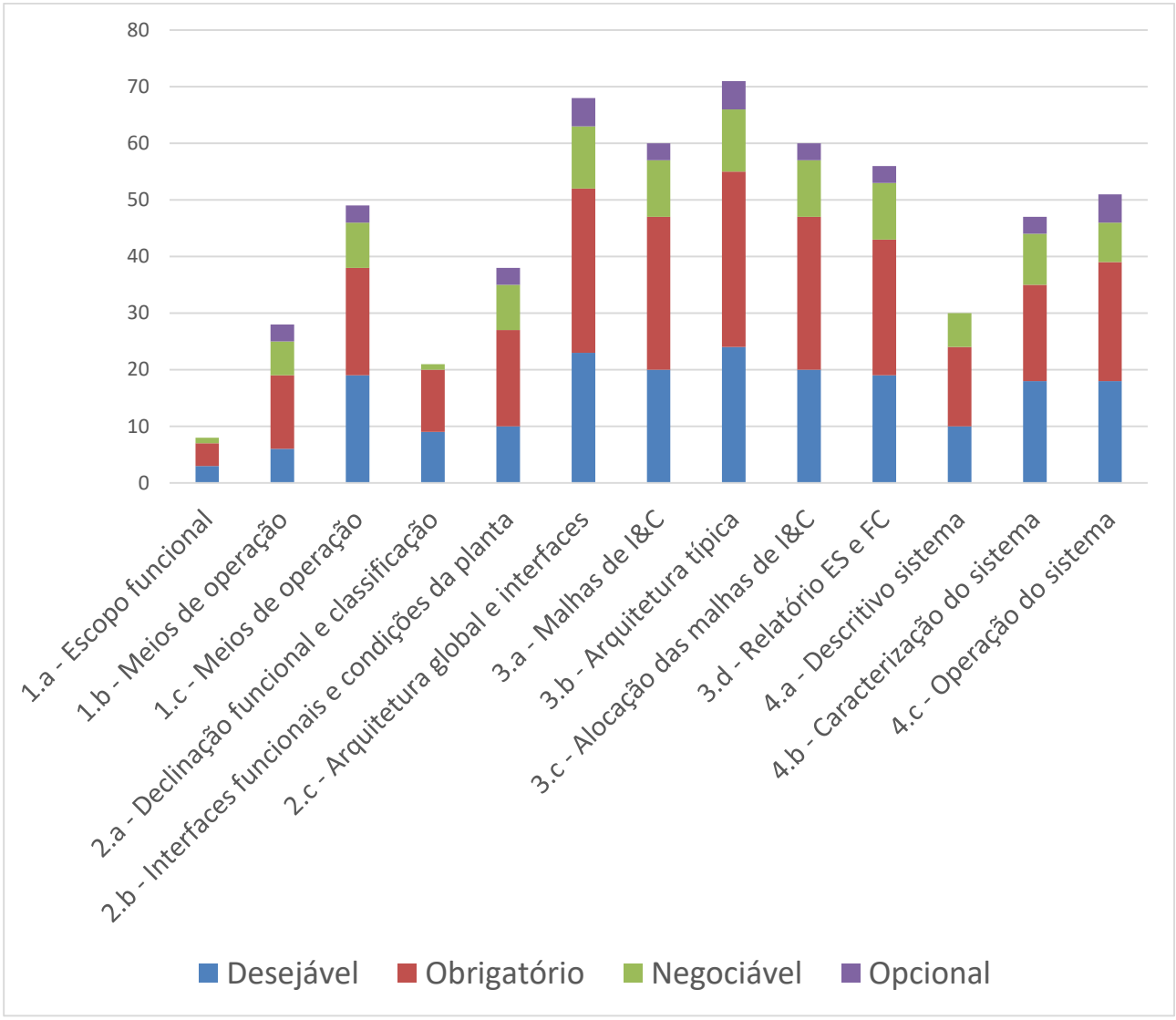


É possível constatar, que a maior parte dos requisitos é aplicada às atividades de arquitetura típica e relatórios ES, o que ratifica o entendimento geral deste estudo. As atividades que decorrem deste grupo, são atividades que estabelecem o "*link*" entre as especificações transversas de alto nível com o nível 4. Cabem a estas também o fluxo de informações entre a ECUNM e EPUNM no nível 4.

O número de requisitos aplicáveis para cada atividade é apresentado na figura 19. No gráfico também foram estratificados as flexibilidades de atendimento dos requisitos (obrigatório, desejável, negociável e opcional). Nota-se que todas as atividades recebem requisitos obrigatórios e negociáveis, o que é fundamental num projeto de sistemas complexos, com vistas à garantia dos princípios da Lei Construtal. Já as atividades de

arquitetura global e típicas (2.c e 3.b) recebem o maior número de requisitos, o que é compreensível por serem atividades que formalizam blocos de função e interfaces. A primeira (2.c) desencadeada pelas especificações de alto nível, a segunda (3.b) com vistas a caracterizar modelos típicos físicos das arquiteturas de I&C no nível 4.

Figura 19 - Estratificação dos requisitos por atividade da metodologia



5 CONCLUSÃO

A identificação da aplicação da lei construtal para avaliar cada decisão tomada na definição e proposição de implementação da metodologia, modelagem dos processos do fluxo das informações, e discriminação das entradas e saídas de dados para alocação da devida responsabilidade e atribuições aos atores envolvidos foi em suma as atividades propostas neste trabalho.

Nesse sentido, foi possível aplicar nestas atividades os requisitos à luz da lei construtal proposta por FREIRE (2018). Dentro do estudo, foi possível ter ciência da interdependência entre os diversos sistemas de uma planta nuclear, logo o registro das decisões à luz da lei construtal se faz necessário. Essa interdependência gera uma maior fonte de complexidade no gerenciamento, consistência e implementação dos dados, e sinais adquiridos e processados pela I&C.

Também foi constatado que estudos vêm sendo feitos para identificar estas dependências (TOMMILA et al., 2016), e como elas podem ser intencionais, ou não. Embora as interações e dependências sejam necessárias e desejáveis, outras não necessárias devem ser identificadas e removidas o mais cedo possível do projeto. Redundância, diversidade e separação são alguns princípios gerais usados para evitar interrelacionamentos desnecessários. Portanto, devem-se estar claro a todos os envolvidos no projeto, os termos e conceitos que relacionam com os objetivos e requisitos dos sistemas de I&C, a estratégia DiD adotada, e as arquiteturas de I&C que estão sendo propostas.

De fato, uma planta nuclear é composta por diversos itens: "*Systems, Structures, and Components*" (SSC), localizados em salas, compartimentos, áreas. Estes itens são conectados um ao outro por diferentes meios (mecânico, fluido, dados, etc.). Para que um SSC opere, ele deve ser suportado por vários itens auxiliares envolvidos em sistemas diversos, tais como suprimento de energia, resfriamento, e controle (RASMUSSEN et al. 1994).

Basicamente, podemos resumir que aos sistemas I&C cabem a coleta dos sinais discretos ou analógicos de cada função de controle individual, a conexão e inter-relacionamento a outras caso necessário. A especificação das funções I&C são implementadas em softwares ("*function block*s") e executadas por equipamentos de controle (controladores distribuídos, centralizados, dispositivos de campo inteligentes)

num modo de evento cíclico ou de batelada. Podemos assim destacar que os SSCs possuem interfaces com:

- Funções próprias: um ou mais sistemas são necessários para executar uma função. Falhas em um SSC afetam o desempenho da função requerida ou causa sua indisponibilidade. SSCs dependem também de sistemas auxiliares. Sistemas auxiliares compartilhados são fontes de Falha de Causa Comum (CCF – *Common Cause Failure*).
- Outros SSCs: Itens da planta intencionalmente conectados por cabos, tubulações, suportações etc. O estado ("*state*": nível de tensão, pressão, temperatura, vibração, etc.) de um componente pode afetar o estado de outro componente.
- Espaço: Condições ambientais (pressão, temperatura, umidade etc.) têm impactos diretos nos itens da planta instalados naquele espaço. Fenômenos físicos originados de outro SSC no mesmo espaço (radiação, vibração, emissão EMC etc.) são transmitidos ao ambiente e outros equipamentos.
- As funções também podem possuir interfaces com outras funções: Interação entre funções na troca de materiais, troca de energia, troca de informação, via uma fonte física (uma memória compartilhada, link de comunicação etc.). Portanto, a execução de funções independentes deve ser sincronizada por eventos.

Conclui-se que o grande desafio em um projeto que envolve sistemas complexos de I&C é o fato de como gerenciar todas as funções de controle, requisitos e interfaces de dados nos ciclos do projeto de forma a reduzir a quantidade de trabalho "braçal". Urge a necessidade de metodologias e ferramentas que coordenem estes desencadeamentos de informações de forma uniforme e rastreável para facilitação do fluxo, tal como a metodologia de especificação proposta neste estudo.

6 CONTRIBUIÇÕES DESTE ESTUDO

Este estudo tem como principal contribuição mostrar a importância da implementação de metodologias baseadas na Lei Construtal em projetos de Sistemas de I&C. Além disso, foi possível apresentar uma metodologia que pode contribuir com o desenvolvimento de ferramentas de engenharia ("*model-based*") que atendam aos requisitos da Lei Construtal.

Portanto, este trabalho pode motivar a comunidade acadêmica a refletir sobre metodologias de projeto e ferramentas que atendam às demandas de projetos complexos dos órgãos governamentais e privados. O estímulo no desenvolvimento de sistemas de engenharia pode inclusive colaborar com outras entidades envolvidas em projetos de sistemas complexos.

Sugere-se um estudo mais aprofundado (estudo de caso) com outros pesquisadores, com o objetivo de especificar e implementar ferramentas de engenharia que contribuam com as entidades envolvidas em projetos de sistemas complexos, fundamentalmente em sistemas de I&C.

Em paralelo, mostra-se necessário a busca por pesquisadores nacionais para o aprofundamento do estudo no campo da Defesa em Profundidade (DiD), visto que esta abordagem auxilia enormemente nas especificações de I&C, como citado ao longo deste estudo. Estudos de DiD com vistas à segurança nuclear sem perder o foco no aumento da confiabilidade de sistemas instrumentados de segurança, disponibilidade e autonomia de plantas nucleares é um enorme campo de pesquisa a ser explorado.

Por fim, a maior dificuldade deste estudo foi não encontrar trabalhos acadêmicos sobre análise funcional e máquinas de estado de plantas nucleares. Publicações acadêmicas neste campo poderiam cooperar significativamente com as especificações de sistemas complexos, incluindo os sistemas de I&C.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, J. B. da M. ***Teoria Geral de Sistemas***. 1. ed. Florianopolis: Instituto Stela. 2012.

AMERICAN NATIONAL STANDARDS INSTITUTE. AMERICAN NUCLEAR SOCIETY. ***Nuclear Safety Criteria For The Design Of Stationary Pressurized Water Reactor Plants.*** Washington: ANSI/ANS, 1988 (ANSI/ANS-51.1).

AMERICAN NATIONAL STANDARDS INSTITUTE. AMERICAN NUCLEAR SOCIETY. ***Safety And Pressure Integrity Classification Criteria For Light Water Reactors.*** Washington: ANSI/ANS, 2017 (ANSI/ANS-58.14).

AMERICAN NATIONAL STANDARDS INSTITUTE. AMERICAN NUCLEAR SOCIETY. ***Time Response Criteria For Manual Actions At Nuclear Power Plants.*** Washington: ANSI/ANS, 2019 (ANSI/ANS-58.8).

AREVA NP Inc. ***U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology***. Lynchburg: *Topical Report*, 2007 (ANP-10284 Rev.0).

AVELLAR, R. K.; & SCHIRRU, R. Applying Humam Factors Engineering Program to the Modernization Project of NPP Control Room in accordance with U.S.NRC and KTA Regulations. ***Brazilian Journal of Radiation Sciences***, 07-02B, 01-10, 2019.

BERTALANFFY, L. V. ***Teoria Geral dos Sistemas:*** Fundamentos, desenvolvimento e aplicações. Petropolis: Vozes. 2008.

CHERNYAEV, A., & ANOKHIN, A. Formalization of the functional analysis methodology to improve NPP I&C design process. In: ANS ANNUAL MEETING AND THE 10TH INTERNATIONAL TOPICAL MEETING ON NUCLEAR PLANT INSTRUMENTATION, CONTROL, AND HUMAN-MACHINE INTERFACE TECHNOLOGIES (NPIC & HMIT), 10th, June 11-15, 2017, San Francisco, CA: USA. **Proceedings...** Disponível em: <http://npic-hmit2017.org/wp-content/data/pdfs/244-20005.pdf> Acesso em: 13 dez. 2019.

CINTRA, R. Otto Hahn – O navio mercante com propulsão nuclear. ***Portal Marítimo***, São Paulo, 12 out. 2016. Disponível em: https://portalmaritimo.com/otto-hahn-o-navio-mercante-com-propulsao-nuclear-que-quase-veio-para-a-mb/. Acesso em 20 jul. 2019.

ELECTRONIC INDUSTRIES ALLIANCE. ***Processes for Engineering a System***. Arlington: EIA, 1999. (EIA-632).

ELECTRIC POWER RESEARCH INSTITUTE. ***Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants.*** Palo Alto: EPRI, 2009. (Technical report 1003567).

ELECTRIC POWER RESEARCH INSTITUTE. ***Principles and Approaches for Developing Overall Instrumentation and Control Architectures that Support***

Acceptance in Multiple International Regulatory Environments. Palo Alto: EPRI, 2014. (Technical report 3002002953).

FREIRE, L. O., & DE ANDRADE, D. A. The Role of Nuclear Power from a System Engineering Standpoint. ***World Journal of Nuclear Science and Technology***, *07* (03), 167-188, 2017.

FREIRE, L. O.; & DE ANDRADE, D. A.; & MONTERRAIN, D. A System Status Definition to Improve Behavior Description in Specifications Based on Constructal Law. ***Open Journal of Applied Sciences***, v. 08, p. 315-337, 2018.

FREIRE, L. O.; & DE ANDRADE, D. A. Constructal Law of Institutions within Social Organizations. ***Open Journal of Applied Sciences***, v. 08, p. 103-125, 2018.

FREIRE, L. O. ***Metodologia de especificação e projeto aplicado a usinas nucleares móveis***. 2018. 180 p. Tese (Doutorado em Tecnologia Nuclear) Instituto de Pesquisas Energéticas e Nucleares, São Paulo. Disponível em: <http://www.teses.usp.br> Acesso em: 10 nov. 2019.

FRUTUOSO E MELO, P. F.; & OLIVEIRA, M. S.; & SALDANHA, LWR Safety Analysis and Licensing and Implications for Advanced Reactors, Nuclear Power - Operation, Safety and Environment. ***Dr. Pavel Tsvetkov (Ed.), ISBN: 978-953-307-507-5, InTech***. p. 47-70, 2011. Disponível em: <https://www.intechopen.com/chapters/17967>. Acesso em 10 ago. 2020.

HALL, A. D. ***A Methodology for Systems Engineering***. 1. ed. Princeton: Van Nostrand Reinhold, 1962.

HASHEMIAN, H.M. Nuclear Power Plant Instrumentation and Control, Nuclear Power - Control, Reliability and Human Factors. ***Dr. Pavel Tsvetkov (Ed.), ISBN: 978-953-307-507-5, InTech***. p. 49-66, 2011. Disponível em: <http://www.intechopen.com/books/nuclear-power-control-reliability-and-human-factors/nuclear-power-plantinstrumentation-and-control>. Acesso em 10 ago. 2020.

HURST, T. (2007). Tow nuclear power I&C out of the 'digital ditch'**.** ***Power magazine,*** London, 15 jan. 2007. Disponível em: < https://www.powermag.com/tow-nuclear-power-ic-out-of-the-digital-ditch>. Acesso em 3 jan. 2020.

INTERNATIONAL ATOMIC ENERGY AGENCY. ***Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook.*** Vienna: IAEA, 1999. (TRS-387).

INTERNATIONAL ATOMIC ENERGY AGENCY. ***Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants***. Vienna: IAEA, 2009. (NP-T-1.5).

INTERNATIONAL ATOMIC ENERGY AGENCY. ***Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants***. Vienna: IAEA (2011). (NP-T-3.12).

INTERNATIONAL ATOMIC ENERGY AGENCY. ***Safety of Nuclear Power Plants: Design***. Vienna: IAEA, 2012. (SSR-2/1).

INTERNATIONAL ATOMIC ENERGY AGENCY. ***Design of Instrumentation and Control Systems for Nuclear Power Plants*.** Vienna: IAEA, 2016. (SSG-39).

INTERNATIONAL ATOMIC ENERGY AGENCY. ***Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants***. Vienna: IAEA, 2018. (NP-T-2.11).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION and THE INTERNATIONAL ELECTROTECHNICAL COMMISSION. ***Systems Engineering — System Life Cycle Processes***. Secretariat: ISO/IEC, 2001. (ISO/IEC 15288).

IEEE POWER ENGINEERING. ***Application and Management of the Systems Engineering Process***. Secretariat: IEEE, 2005. (IEEE 1220).

LANGE, R. S. ***Theme Study – Large Vessel NS Savannah***. 1990. 32 p. U.S. Department of the Interior, History Division, Washington, DC.

LEOCARDIO, M. S. (2020). ***Análise do formato de apresentação das dissertações do Programa de Pós-Graduação do Instituto de Pesquisas Energéticas e Nucleares - IPEN***. 2020. 64 p. Dissertação (Mestrado em Tecnologia Nuclear) Instituto de Pesquisas Energéticas e Nucleares, IPEN-CNEN/SP, São Paulo. Disponível em: <http://www.teses.usp.br> Acesso em: 21 jul. 2021.

LIPTÁK, B. G. (2006). ***Safety Instrumentation & Justification of Its Cost, Instrument Engineers' Handbook.*** 4. ed. Boca Raton: Taylor & Francis, 2006.

MARI, C. ***Hedging electricity price volatility using nuclear power*.** Applied Energy , 113, 615-621, 2014.

MCMAHON, T. ***Historical Crude Oil Prices (Table)***. Retrieved Setember 10, 2017, Disponível em: <https://inflationdata.com/Inflation/Inflation_Rate> Acesso em: 10 jul. 2021.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION. ***NASA Systems Engineering Handbook.*** Washington: NASA, 2007. (NASA/SP-2007-6105 Rev1). Disponível em: <https://www.nasa.gov/> Acesso em: 10 nov. 2019.

NAKAO, M.: Radiation Leaks from Nuclear Power Ship "Mutsu". 1992. Disponível em: <http://www.sozogaku.com/fkd/en/cfen/ CA1000615.html> Acesso em: 23 dez. 2019.

NUCLEAR REGULATORY COMMISSION. ***Definitions.*** Washington: U.S. NRC, 2020a. (10 CFR 20.1003).

NUCLEAR REGULATORY COMMISSION. ***General Design Criteria for Nuclear Power Plants.*** Washington: U.S. NRC, 2020b. (10CFR50: Appendix A).

NUCLEAR REGULATORY COMMISSION. ***Environmental qualification of electric equipment important to safety for nuclear power plants.*** Washington: U.S. NRC, 2020c. (10CFR50.49).

NUCLEAR REGULATORY COMMISSION. ***Human Factors Engineering Program Review Model.*** Washington: U.S. NRC, 2012. (NUREG-0711, Revision 3).

NUCLEAR REGULATORY COMMISSION. ***Human-System Interface Design Review Guidelines.*** Washington: U.S. NRC, 2020d. (NUREG-0700, Revision 3).

NUCLEAR REGULATORY COMMISSION. ***Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition.*** Washington: U.S. NRC, 2021. (NUREG-0800).

NUCLEAR REGULATORY COMMISSION. ***Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems.*** Washington: U.S. NRC, 1994. (NUREG/CR-6303).

NUCLEAR REGULATORY COMMISSION. ***Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems.*** Washington: U.S. NRC, 2009. (NUREG/CR-7007).

OFFICE OF SHIP DISPOSAL - MARITIME ADMINISTRATION. ***N.S. Savannah Updated Final Safety Analysis Report***. Washington: U.S. Department of Transportation, 2011. *(STS-004-002).*

O'ROURKE, R. ***Navy Nuclear-Powered Surface Ships: Background, Issues, and Options for Congress***. 2010. Congressional Research Service, United States of America.

ROYAL ACADEMY OF ENGINEERING. **Future Ship Powering Options Exploring alternative methods of ship propulsion**. Royal Academy of Engineering. United. 2013.

RASMUSSEN, J.; & PEJTERSEN, A. & GOODSTEIN, L. P. ***Cognitive systems engineering***. New York: Wiley. 1994.

STANDARDS COUNCIL OF CANADA. ***Systems Engineering – Guide for ISO/IEC 15288 (System Life Cycle Processes).*** Quebec: SCC, 2002. Disponível em: <https:// www.scc.ca> Acesso em: 3 mar. 2020.

SUMMERS, A. E. ***Safety Instrumentation Systems***. Houston: Sis-Tech - Perry's Handbook of Chemical Engineering, Edition Fall. 2007.

WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION. ***Safety of new NPP designs - Study by Reactor Harmonization Working Group RHWG***. WENRA, 2013. Disponível em: <http:// www.wenra.eu/publications> Acesso em: 13 jun. 2020.

WORLD NUCLEAR ASSOCIATION. ***Safety Classification for I&C in Nuclear Power Plants – Current Status & Difficulties, Cooperation in Reactor Design Evaluation and Licensing Digital Instrumentation and Control Task Force.*** London: WNA, 2015. Disponível em: <http://www.world-nuclear.org> Acesso em: 13 jun. 2020.

WORLD NUCLEAR ASSOCIATION. ***International Nuclear I&C and Electrical System Standards List with URLs.*** London: WNA, 2020. Disponível em: <http://www.world-nuclear.org> Acesso em: 13 jun. 2020.

THOMSON, J. ***Nuclear Power Station Control and Instrumentation Safety Systems Architecture:*** An Overview. London: Safety in Engineering, 2012.

TOMMILA, T. & PAPAKONSTANTINOU, NIKOLAOS, N. **Challenges in Defence in Depth and I&C architectures**. Tampere: Research Report VTT, 2016.

ANEXO 1 – Terminologias e conceitos relativos à engenharia de sistema

A tabela 8 tem como propósito harmonizar a terminologia utilizada neste trabalho, em conformidade com a tese de FREIRE (2018). Outros conceitos não catalogados na tese de FREIRE (2018) foram complementados para sustentar este trabalho.

Tabela 8 - Terminologia de I&C

Termo	**Descrição**	**Pode ser decomposto em**	**Tem ou pode ter**	**Pode acarretar**
Sistema	Divisão do universo em duas partes (interior e exterior), sendo que o interior realiza funções de serviço para exterior e precisa receber serviços do mesmo	-Elementos: Componentes ou Sistema	- Função - Status - Fase	- Falta - Mau funcionamento
Elementos sistêmicos	Elementos que compõe o sistema	- componentes - subsistemas	- Função - Mau funcionamento (falta)	-
Status sistêmico	Combinação simultânea dos status de todas as funções trocadas entre o interior e o exterior de um sistema ou série de informações trocadas que configuram o status de um sistema.	- Identificação do sistema (tag) - Nome do status - Lista de status do sistema (de serviço e recebidas)	- Status de cada função	-
Fase sistêmica (ou transição)	Um evento de mudança de um dado status A para outro dado status B dentro de um período finito e determinado no tempo	- Fase ativa - Fase passiva	-	-

Termo	Descrição	Pode ser decomposto em	Tem ou pode ter	Pode acarretar
Fase ativa	O sistema precisa mudar o status de alguma função técnica	-	-	-
Fase passiva	O sistema não necessita de qualquer ação interna, depende apenas de ações externas (funções recebidas)	-	-	-
Falta (fault) *	Causa da inabilitação de um elemento de cumprir sua função	- Defeito - Erro	-	- Falha - Mau funcionamento
Defeito (defect.) *	Um tipo de falta causada por uma discrepância na estrutura estática do elemento de um sistema (mais relacionado ao “hardware”)	-	-	- Falha - Mau funcionamento
Erro (error) *	Um tipo de falta causada por uma discrepância no estado dinâmico de um elemento de um sistema (mais relacionado ao “software”)	-	-	- Falha - Mau funcionamento
Falha (failure) *	Evento de inabilitação de elemento do sistema de não efetuar sua função	- Falha de Causa Comum - Falha Múltipla	-	- inabilitação de uma ou mais funções
Mau funcionamento (Malfunction) *	Comportamento visível imprevisto causado pela falta de um sistema ou componente.	- Caracterizado pelo modo de falha	- É identificado quando há demanda - Pode ser prevenido com critérios de tolerância a falta	- Falha mecânica

Termo	Descrição	Pode ser decomposto em	Tem ou pode ter	Pode acarretar
Modo de falha (failure mode) *	Tipo de mau funcionamento usado para caracterização de diferentes tipos de maus funcionamentos, tais como: perda da função, saída errada ou sinal perdido.	-	-	-
Demanda (demand) *	Uma requisição de um serviço via comando externo.	-	-	- Funcionamento - Mau funcionamento
Função	Objetivo ou ação física desejada que o sistema dever efetuar. É uma descrição do que deve ser feito.	- Status - Relevância	-	-
Status funcional	Situação possível de execução com determinado conjunto de desempenhos ou prontidão com determinado tempo de resposta, assumindo a cada momento um único valor dentro de uma lista finita.	- Função ativa - Função inativa - Função em prontidão - Função inibida	-	-
Função ativa (active function)	Sistema efetua determinado serviço com certo desempenho – status de performance (nominal, parcial, parcial 50%, parcial 75%, etc.)	-	-	-
Função inativa	Parada ou indisponibilidade de um serviço sem previsão de retorno.	-	-	-
Função em prontidão	Sistema pronto para iniciar determinado serviço num prazo ou ocorrência de determinado evento	-	-	-

Termo	Descrição	Pode ser decomposto em	Tem ou pode ter	Pode acarretar
Função inibida	Inibição de determinada ação ou serviço para evitar acidentes	-	-	-
Relevância funcional	Uma dada função de serviço ou recebida é relevante para a determinação do status se ela muda de status durante a operação do sistema e pelo menos uma das condições abaixo for verdadeira: 1 – O custo adicional que esta função cria ao projeto do sistema em termos de dimensionamento ou equipamento é significativo; 2 – O custo esperado causado pelos acidentes devido à sua falha ou atuação inadvertida é significativo.	-	-	-
Funções de controle ou controle	São funções que executam ações em determinados componentes, sejam elas para operar (comandar) ou supervisionar (monitorar).	- Controle automático - Controle manual	- Falta - Mau funcionamento	-
Controle automático	São funções de controle executadas somente pelo solucionador lógico eletrônico sem a intervenção humana	- Regulagem contínua - Intertravamento	-	-
Controle manual	São funções de controle executadas com intervenção humana	-	-	-

Fonte: adaptado de FREIRE (2018) e TOMILA (2016).

ANEXO 2 – Lista de requisitos e suas justificativas

A tabela 9 tem como propósito estabelecer uma relação N para N entre as atividades proposta por este estudo e os requisitos da lei construtal da tese de FREIRE (2018). Em cada linha da tabela é apresentado o requisito da lei construtal, a flexibilidade de atendimento (obigatório, negociável, desejável e opcional), a relação com as atividades deste trabalho, e a devida justificativa.

Tabela 9 - Matriz de atendimento aos requisitos à Luz da Lei Construtal

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
1	Identificando subsistemas - As especificações de subsistemas serão em forma de caixa preta.	Obrigatório	X	X	X											É prevista a identificação dos subsistemas em blocos, para que o ruído seja reduzido e a qualidade do trabalho melhorada sem que haja um aumento de trabalho, requerendo apenas disciplina das pessoas.
2	Identificando subsistemas - A especificação deve identificar todos os subsistemas.	Obrigatório	X	X	X	X	X	X								É prevista a identificação de todos os subsistemas, para preservar a integridade das informações necessárias ao projeto de um sistema.
3	Identificando subsistemas - A análise de cima para baixo deverá escolher a opção com o menor custo.	Desejável	X	X	X	X	X	X	X	X	X	X	X	X	X	É prevista a análise de cima para baixo e escolha da opção com o menor custo, para a redução de custo do ruído.
4	Identificando funções - A especificação deve identificar todas as funções de cada subsistema.	Obrigatório	X	X	X	X	X	X	X	X	X		X			É prevista a identificação de todas as funções importantes para segurança, para preservar a integridade das informações necessárias ao trabalho.
5	Identificando funções - Toda função deve ser composta por verbo e talvez por objetos direto ou indiretos, com a seguinte forma: [verbo] {objeto direto} {objeto indireto}.	Obrigatório	X			X							X			A descrição (especificação) funcional do sistema conforme apresentada no requisito garantirá a facilitação do fluxo de informações.
6	Identificando funções - As funções recebidas pelo sistema devem ser desmembradas em funções técnicas.	Desejável				X							X			As funções especificadas pelo nível imediatamente superior prevê desmembramento em funções técnicas, para facilitar o fluxo de informação, evitando que seja necessário mudar a especificação de nível superior.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
7	Identificando funções - Para cada função, a especificação deve identificar um único sistema responsável.	Obrigatório				X	X	X	X	X	X	X	X			Cada função técnica prevê alocação a um sistema específico, para facilitar o fluxo de informação entre os níveis hierárquicos.
8	Identificando funções - Para cada função, a especificação deve identificar os sistemas alvos.	Obrigatório				X	X	X	X	X	X	X	X			A especificação de cada função técnica prevê registro do sistema que recebe o serviço. O trabalho de especificação precisa registrar quais subsistemas recebem cada função para posteriormente identificar os status de subsistema.
9	Identificando funções - Um dado subsistema deve realizar funções técnicas com propriedades similares.	Negociável				X	X	X	X	X	X	X		X		A análise funcional contemplada na arquitetura prevê realização de categorização/classificação de segurança das funções, para manter a integridade das informações relevantes.
10	Identificando funções - Funções técnicas com confiabilidade elevada devem permanecer em prontidão nos status normais.	Desejável				X	X	X	X	X	X	X			X	A especificação de operação do sistema deverá contemplar as funções técnicas com vias a confiabilidade dos sistemas em prontidão, para facilitar o fluxo de produção de informação.
11	Definindo nexos causais - A especificação deve identificar o nexo causal entre funções de serviço e funções técnicas.	Obrigatório				X	X	X	X	X	X		X			Nas arquiteturas típicas, devem ser levantados os requisitos que deverão ser declinados a cada desmembramento funcional, para obter uma solução, facilitando o fluxo de informação.
12	Definindo nexos causais - A especificação deve identificar o nexo causal entre as propriedades do sistema e suas funções técnicas.	Obrigatório				X	X	X	X	X	X			X		A especificação dos requisitos declinados deve levar em consideração conceitos e critérios de I&C contempladas na base normativa nuclear e complementares, para manter a integridade das informações relevantes.
13	Classificando funções técnicas - Para cada subsistema, a especificação deve definir quais funções técnicas são relevantes.	Desejável				X							X		X	A categorização/classificação de segurança deverá prever meios de identificar SSCs relevantes ou irrelevantes, implementar taxonomia e codificação de cores específica para facilitar a classificação das funções técnicas, para manter a integridade das informações relevantes.
14	Identificando status - A especificação deve definir os possíveis status de cada função técnica.	Obrigatório				X							X		X	O processo de categorização/ classificação deverá conter especificação dos possíveis status de cada função técnica, para reduzir o ruído na comunicação.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
15	Identificando status - Para cada status do sistema, a especificação deve definir os status de cada função técnica.	Obrigatório							X	X	X	X	X		X	Na identificação e especificação de status, para cada status do sistema, a especificação deve definir os status de cada função técnica, sendo que as funções podem estar ativas, em prontidão, inativas ou até inibidas, e as funções irrelevantes não precisam ter uma definição de status, para manter a integridade das informações relevantes.
16	Identificando status - A especificação deve identificar todas as combinações de status das funções relevantes de cada subsistema.	Obrigatório							X	X	X	X	X		X	A análise funcional, deve definir os status de cada função técnica, para facilitar a avaliação e verificação do trabalho, facilitando a comunicação com revisores.
17	Identificando status - Todo status de subsistema deve ser único.	Desejável							X	X	X	X	X		X	Na especificação operacional, deve se assegurar que os status sejam únicos, verificando se existem maneiras de interação idênticas usando a tabela de atividade das funções internas, para preserva a integridade da informação relevante.
18	Identificando fases - Para cada fase ativa do sistema, a especificação deve identificar as fases necessárias dos subsistemas.	Obrigatório							X	X	X	X	X		X	Para cada fase ativa do sistema, a especificação deve identificar as fases necessárias dos subsistemas, pois o trabalho de identificação e especificação de transições preserva a integridade das informações relevantes ao projeto.
19	Identificando fases - A especificação deve classificar as fases em ativas ou passivas.	Desejável							X	X	X	X	X		X	A especificação deve classificar as fases em ativas ou passivas, pois reduz ruído e esforço global durante a atividade de especificação de subsistemas.
20	Declinando requisitos - Para cada propriedade do sistema, a especificação deve definir se existe relação com cada propriedade dos subsistemas.	Obrigatório			X			X	X	X	X	X		X		Para preservar a integridade de informações essenciais ao projeto dos subsistemas.
21	Declinando requisitos - A especificação deve traduzir os requisitos não funcionais do sistema em requisitos não funcionais dos subsistemas.	Obrigatório			X			X	X	X	X	X		X		Para preservar a integridade de informações essenciais ao projeto dos subsistemas.
22	Declinando requisitos - Requisitos não-funcionais serão uma relação de uma propriedade do com uma condição.	Obrigatório			X			X	X	X	X	X		X		A caracterização deve evitar a redação de requisitos subjetivos, sob pena de introduzir entraves na escrita, para preservar a integridade de informações essenciais ao projeto dos subsistemas, de forma a evitar a introdução de ruído no processo.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
23	Declinando requisitos - Requisitos não-funcionais devem definir as condições ambientais que os subsistemas devem suportar.	Negociável			X			X	X	X	X	X		X		Requisitos não-funcionais devem definir as condições ambientais para preservar a integridade das informações necessárias ao projeto de um sistema: faixa de temperatura, de pressão atmosférica e de humidade do ambiente, vibração, choque, inclinação, movimentos, presença de pó e presença de água, para preservar a integridade das informações necessárias ao projeto de um sistema.
24	Declinando requisitos - Requisitos não-funcionais devem definir as resistências aos riscos externos.	Desejável			X			X	X	X	X	X		X		Requisitos não-funcionais devem definir as resistências aos riscos externos para preservar a integridade das informações necessárias ao projeto: alagamento, terremoto, furacão, impacto e incêndio, para preservar a integridade das informações necessárias ao projeto de um sistema.
25	Declinando requisitos - A especificação deve criar requisitos não funcionais limitando o tempo de operação em cada estado.	Desejável			X			X	X	X	X	X		X	X	A especificação deve criar requisitos não funcionais limitando o tempo de operação em cada estado, para assegurar que os cálculos de confiabilidade sejam realistas, contribuindo para manter a integridade de informações relevantes.
26	Declinando requisitos - Requisitos não funcionais serão relacionados aos status do subsistema.	Desejável			X			X	X	X	X	X		X	X	Requisitos não funcionais serão relacionados aos status do subsistema, fazendo um projeto sem superdimensionamento, contribuindo para manter a integridade de informações relevantes.
27	Declinando requisitos - Pelo menos um requisito de verificação deve refinar todo requisito não funcional.	Desejável			X			X	X	X	X	X		X		Pelo menos um requisito de verificação deve refinar todo requisito não funcional para manter a integridade de informações relevantes.
28	Caracterizando status - A especificação deve traduzir os requisitos das funções de serviço em requisitos das funções técnicas.	Obrigatório			X			X	X	X	X	X		X	X	A caracterização deve traduzir as demandas para que o sistema atenda aos requisitos, e assim preservar a integridade das informações relevantes ao projeto.
29	Caracterizando status - A especificação deve traduzir os requisitos não funcionais do sistema em requisitos das funções técnicas.	Obrigatório			X			X	X	X	X	X		X	X	A caracterização deve traduzir as demandas para que o sistema atenda aos requisitos, e assim preservar a integridade das informações relevantes ao projeto.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
30	Caracterizando status - Requisitos devem ser compreensíveis pelo receptor.	Obrigatório			X			X	X	X	X	X		X	X	A especificação precisa prover adequada comunicação com os representantes de fornecedores que não tem a mesma cultura, linguagens ou vocabulários estranhos ao fornecedor devem ser evitadas. Ao entrar em contato com pessoas de diferente cultura, algumas pessoas tendem a entrar em conflito ou cometer enganos. Este requisito advém da necessidade de facilitar a comunicação.
31	Caracterizando status - Para cada par função técnica e status no qual a função técnica está ativa, a especificação deve vincular pelo menos um requisito de desempenho.	Desejável			X			X	X	X	X	X		X	X	A caracterização prevê a definição de requisitos de desempenho por status leva a soluções mais eficientes porque variam de status para status.
32	Caracterizando status - A especificação deve vincular pelo menos um requisito de desempenho a cada função irrelevante.	Desejável			X			X	X	X	X	X		X	X	A caracterização prevê ao menos um requisito para cada função irrelevante para preservar a integridade das informações relevantes ao projeto.
33	Caracterizando status - Para cada par função técnica e status no qual a função técnica está em prontidão, a especificação deve vincular pelo menos um requisito de resposta temporal	Desejável			X			X	X	X	X	X		X	X	A caracterização prevê resposta temporal de acionamento de funções por ser um aspecto dimensionante para alguns componentes e para preservar a integridade das informações relevantes ao projeto.
34	Caracterizando status - Para cada par função técnica e status no qual a função técnica está inibida, a especificação deve vincular pelo menos um requisito de máxima frequência de atuação inadvertida.	Obrigatório			X			X	X	X	X	X		X	X	A caracterização prevê o requisito, e embora este trabalho de análise de segurança seja adicionado, ele contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.
35	Caracterizando status - Pelo menos um requisito de taxa de falha deve refinar todo requisito de desempenho.	Negociável			X			X	X	X	X	X		X	X	A caracterização prevê o requisito, e embora este trabalho de análise de segurança seja adicionado, ele contribui para preservar a integridade de informações essenciais ao projeto dos subsistemas.
36	Caracterizando status - Pelo menos um requisito de taxa de reparo deve refinar todo requisito de taxa de falha.	Negociável			X			X	X	X	X	X		X	X	A caracterização prevê o requisito de MTTR, para preservar a integridade de informações essenciais ao projeto dos subsistemas.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
37	Caracterizando status - Um requisito de probabilidade de falha sob demanda deve refinar todo requisito de resposta temporal.	Desejável			X			X	X	X	X	X		X	X	A caracterização prevê o requisito de falha sob demanda, para preservar a integridade de informações essenciais ao projeto dos subsistemas.
38	Caracterizando status - Especificações devem ser listas de requisitos atômicos numerados.	Desejável			X			X	X	X	X	X		X	X	A caracterização prevê requisitos atômicos no sentido que eles devem ter uma única ideia (relaciona uma propriedade com uma condição) com todos seus qualificadores necessários, para facilitar a comunicação durante todo o projeto.
39	Caracterizando status - Propriedades podem ser grandezas com unidade de medida.	Opcional			X									X		A caracterização prevê o requisito de com respectivas propriedades, para eliminar erros de comunicação ao longo de todo o projeto.
40	Caracterizando status - Propriedades podem ser uma opção dentro de uma lista pré-definida.	Opcional			X									X		A caracterização prevê lista de propriedades para os requisitos, para eliminar erros de comunicação ao longo de todo o projeto.
41	Caracterizando status - Propriedades podem ter complementos nominais ou adjetivos.	Opcional			X									X		A caracterização prevê o requisito de com respectivas propriedades, para eliminar erros de comunicação ao longo de todo o projeto.
42	Caracterizando status - Pelo menos um requisito de verificação deve refinar todo requisito de desempenho.	Desejável			X			X						X		A caracterização prevê o requisito de com refinos em relação ao desempenho, para eliminar erros de comunicação ao longo de todo o projeto.
43	Caracterizando status - Todo requisito de verificação deve definir o método de verificação.	Desejável		X	X	X	X	X	X	X	X	X	X	X	X	A caracterização prevê o método de verificação, para preservar a integridade de informações essenciais ao projeto dos subsistemas.
44	Caracterizando status - Todos os requisitos devem ser refinados por um requisito de flexibilidade.	Obrigatório		X	X	X	X	X	X	X	X	X		X	X	A caracterização prevê flexibilidade de atendimento ao requisito, para reduzir o ruído no processo.
45	Caracterizando status - Em um requisito, a flexibilidade será proporcional ao risco de inviabilidade.	Obrigatório		X	X	X	X	X	X	X	X	X		X	X	A caracterização prevê flexibilidade em relação ao risco de inviabilidade, para que o projeto avance rapidamente com abertura à inovação, facilitando a comunicação enquanto o ruído gerado por requisitos inviáveis é reduzido.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
46	Caracterizando status - Os requisitos classificados como obrigatórios devem ser viáveis tanto individualmente como coletivamente.	Obrigatório		X	X	X	X	X	X	X	X	X		X	X	A caracterização prevê classificação dos requisitos, para reduzir o ruído no processo.
47	Escolhendo método - Para cada subsistema, a especificação deve escolher o método de obtenção (projeto interno, projeto externo, prateleira).	Obrigatório			X			X	X	X	X	X		X		A caracterização prevê a escolha do método de especificação, para facilitar o fluxo de informação.
48	Caracterizando interfaces - Se um subsistema for reusado, a especificação deve incluir requisitos das interfaces aplicados aos subsistemas adjacentes.	Desejável	X	X	X	X	X	X	X	X	X	X	X	X	X	O descritivo prevê reuso de subsistemas, para facilitar o fluxo de informação por reduzir os custos.
49	Caracterizando interfaces - A especificação deve declarar a autoridade de projeto das interfaces.	Negociável	X				X	X		X			X			O descritivo prevê a declaração das autoridades de projeto, para preserva a integridade de dados, evitando prejuízos.
50	Compatibilizando interfaces - Sempre que necessário, o projeto deverá revisar a arquitetura do sistema.	Desejável	X	X	X	X	X	X	X	X	X		X			A categorização funcional prevê a revisão da arquitetura, para facilitar o fluxo de informação no projeto.
51	Compatibilizando interfaces - O projeto deve empregar subsistemas sob a forma de caixa preta.	Desejável				X	X	X		X			X		X	As interfaces funcionais preveem implementação em blocos para reduzir o ruído.
52	Compatibilizando interfaces - O projeto deve compatibilizar os requisitos de interface dos componentes.	Obrigatório						X		X			X			O descritivo prevê a declaração das interfaces e a compatibilização dos respectivos requisitos, para facilitar o fluxo de informação durante o projeto.
53	Definindo modos de operação - Variáveis e modos de operação de componentes devem permitir o reconhecimento imediato do modo de operação do produto.	Desejável						X		X					X	O descritivo operacional prevê as variáveis e modos de operação, para facilitar o fluxo de informação através do produto, o que atende ao enunciado da lei construtal.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
54	Definindo modos de operação - O projeto deverá definir as configurações físicas permitidas para cada modo.	Desejável						X		X					X	O descritivo operacional prevê as configurações físicas, para reduzir a entrada de informação falsa no projeto, melhorando o fluxo de informação.
55	Definindo modos de operação - O projeto deverá identificar as configurações físicas proibidas, se houver.	Obrigatório						X		X					X	O descritivo operacional identifica as configurações físicas proibidas, para assegurar que informações relevantes sejam preservadas durante um projeto, melhorando o fluxo de informações.
56	Definindo modos de operação - Os modos de operação devem atender a todos os status.	Obrigatório						X		X					X	O descritivo operacional prevê que os modos atendam os status, para eliminar muitos riscos e contratempos na fase de integração por manter a integridade das informações relevantes.
57	Definindo modos de operação - Mais de um modo pode atender um dado status.	Opcional						X		X					X	O descritivo operacional prevê que mais de um modo atenda um status, para eliminar muitos riscos e contratempos na fase de integração por manter a integridade das informações relevantes.
58	Definindo modos de operação - Um modo pode atender vários status.	Opcional						X		X					X	O descritivo operacional prevê que um modo atenda vários status, para reduzir o número de modos de operação e procedimentos, evitando ruído.
59	Definindo configurações - O projeto deve definir as configurações físicas de referência.	Obrigatório						X		X					X	A arquitetura típica configurações físicas de referência, para reduzir o ruído no projeto por uniformizar as hipóteses de cálculo.
60	Definindo configurações - A justificativa de inclusão de uma configuração física de referência deve ser verificação de dimensionamento de componentes.	Desejável			X			X		X				X		A caracterização prevê justificativas de configurações físicas, para reduzir as configurações físicas ao mínimo necessário contribui para reduzir o ruído.
61	Calculando desempenhos - O projeto deve estimar o desempenho das funções para cada configuração física de referência.	Obrigatório			X		X	X	X	X	X	X		X		A caracterização prevê justificativas de configurações físicas, para preservar a integridade de informação relevante ao longo do projeto.
62	Calculando desempenhos - O projeto deve estimar a confiabilidade das funções para cada configuração física de referência.	Desejável			X		X	X	X	X	X	X		X		A caracterização prevê a estimativa da confiabilidade funcional, para preservar a integridade de informação relevante ao longo do projeto.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
63	Calculando desempenhos - O projeto deve estimar a taxa de reparo das funções para cada configuração física de referência.	Desejável			X		X	X	X	X	X	X		X		A caracterização prevê a estimativa da taxa de reparo, para preservar a integridade de informação relevante ao longo do projeto.
64	Definindo transições - O modo de operação medido deverá guiar o comportamento do produto.	Negociável		X			X	X	X	X	X	X		X		A caracterização prevê o modo de operação seja medido, para facilitar o fluxo de informação durante a vida do produto por reduzir ao ruído de processo na forma de ordens e comandos incoerentes com a realidade.
65	Definindo transições - O projeto deve prever pelo menos um procedimento por fase ativa.	Obrigatório		X			X	X	X	X	X	X			X	O descritivo operacional prevê pelo menos um procedimento por fase, para eliminar muitos riscos e contratempos na fase de integração por manter a integridade das informações relevantes.
66	Definindo transições - Se o mesmo modo realiza os status de início e fim de uma fase, tal fase não precisa de um procedimento.	Opcional		X			X	X	X	X	X	X			X	O descritivo operacional prevê a não necessidade de determinada fase, para simplificar o projeto, reduzindo ruído.
67	Definindo transições - A definição de procedimentos pode requerer a definição de novos status.	Opcional		X			X	X	X	X	X	X			X	O descritivo operacional prevê a definição de novos status, para melhorar a rapidez com que o projeto avança, facilitando o fluxo de informações.
68	Definindo transições - Um procedimento pode realizar várias fases.	Opcional		X			X	X	X	X	X	X			X	O descritivo operacional prevê que um procedimento pode realizar vária fases, para simplificar o projeto, reduzindo ruído.
69	Definindo transições - O projeto deve definir cada procedimento como sequência de procedimentos dos componentes ou sistemas externos.	Obrigatório		X			X	X	X	X	X	X			X	O descritivo operacional prevê sequenciamento de procedimentos, para simplificar o projeto, reduzindo ruído.
70	Definindo transições - O projeto deve demonstrar que todo procedimento respeita as configurações físicas permitidas.	Obrigatório		X			X	X	X	X	X	X			X	A caracterização prevê demonstração de que os procedimentos respeitam as configurações físicas, para reduzir a propagação de ruído na forma de comportamentos (operação) ou arquitetura inadequados dos produtos.
71	Projetando interfaces - O projeto deverá definir requisitos de interface.	Desejável		X	X	X	X	X	X	X	X	X		X		A caracterização prevê requisitos de interface, para manter a integridade das informações relevantes.
72	Projetando interfaces - A observabilidade deve ser compatível com os riscos de operação.	Negociável		X	X		X	X	X	X	X	X	X		X	O descritivo operacional prevê a observalidade dos riscos operacionais, para reduzir o ruído.

Item	Requisito Freire		Atividades deste trabalho													Justificativa
			1.a	1.b	1.c	2.a	2.b	2.c	3.a	3.b	3.c	3.d	4.a	4.b	4.c	
73	Analisando riscos - O projeto deverá gerenciar riscos criados pelos componentes.	Negociável		X	X		X	X	X	X	X	X	X	X	X	A caracterização prevê gerenciamento de riscos, para facilitar o fluxo de informações
74	Analisando riscos - O projeto deverá declarar os riscos internos do produto em termos de natureza, gravidade, efeitos nas interfaces e frequência.	Obrigatório		X	X		X	X	X	X	X	X	X	X	X	A caracterização prevê a declaração de riscos, para preservar as informações relevantes.
75	Analisando riscos - O projeto deve analisar os riscos para cada passo dos procedimentos.	Negociável		X	X		X	X	X	X	X	X	X	X	X	A caracterização prevê a análise de riscos, para preservar as informações relevantes.
76	Calculando propriedades - Caso o projeto tenha mudado a arquitetura do produto, o projeto deve recomeçar desde o começo.	Obrigatório		X	X		X	X	X	X	X	X	X	X	X	O descritivo prevê a reconfiguração total do projeto, para evitar inconsistências, reduzindo o ruído do processo na forma de dados errados como resultado do projeto.
77	Calculando propriedades - Balanços devem calcular intervalos de confiança das estimativas.	Desejável		X	X		X	X	X	X	X	X	X	X	X	A caracterização prevê nos balanços os intervalos de confiança de estimativas, para que a ineficiência do ponto de vista da lei construtal e possa ser evitada com a preservação da informação de intervalos de confiança.
78	Calculando propriedades - O projeto deverá definir rotinas de manutenção e reparo em termos de natureza e duração.	Negociável		X	X		X	X	X	X	X	X	X	X	X	A caracterização prevê as rotinas de manutenção, para manter a integridade de uma informação relevante que são os dados de entrada para calcular a disponibilidade do produto.
79	Verificando atendimento - O projeto deve preencher a matriz de atendimento.	Obrigatório		X	X		X	X	X	X	X	X	X	X	X	A caracterização prevê a matriz de atendimento, para verificar o trabalho, sendo uma grande solução para facilitar o fluxo de informação.
80	Verificando atendimento - O projeto deverá verificar o cumprimento dos requisitos não funcionais.	Obrigatório		X	X		X	X	X	X	X	X	X	X	X	A caracterização prevê o cumprimento dos requisitos, para facilitar a tomada de decisões.
81	Verificando atendimento - A matriz de atendimento deverá incluir a probabilidade de atendimento dos requisitos obrigatórios.	Negociável		X	X		X	X	X	X	X	X	X	X	X	A caracterização prevê a probabilidade de atendimento, para facilitar a tomada de decisões.

Fonte: adaptado de FREIRE (2018).

ANEXO 3 – Correlação de classificações e condições da planta

Figura 20 - Correlação - CSN e condições da planta

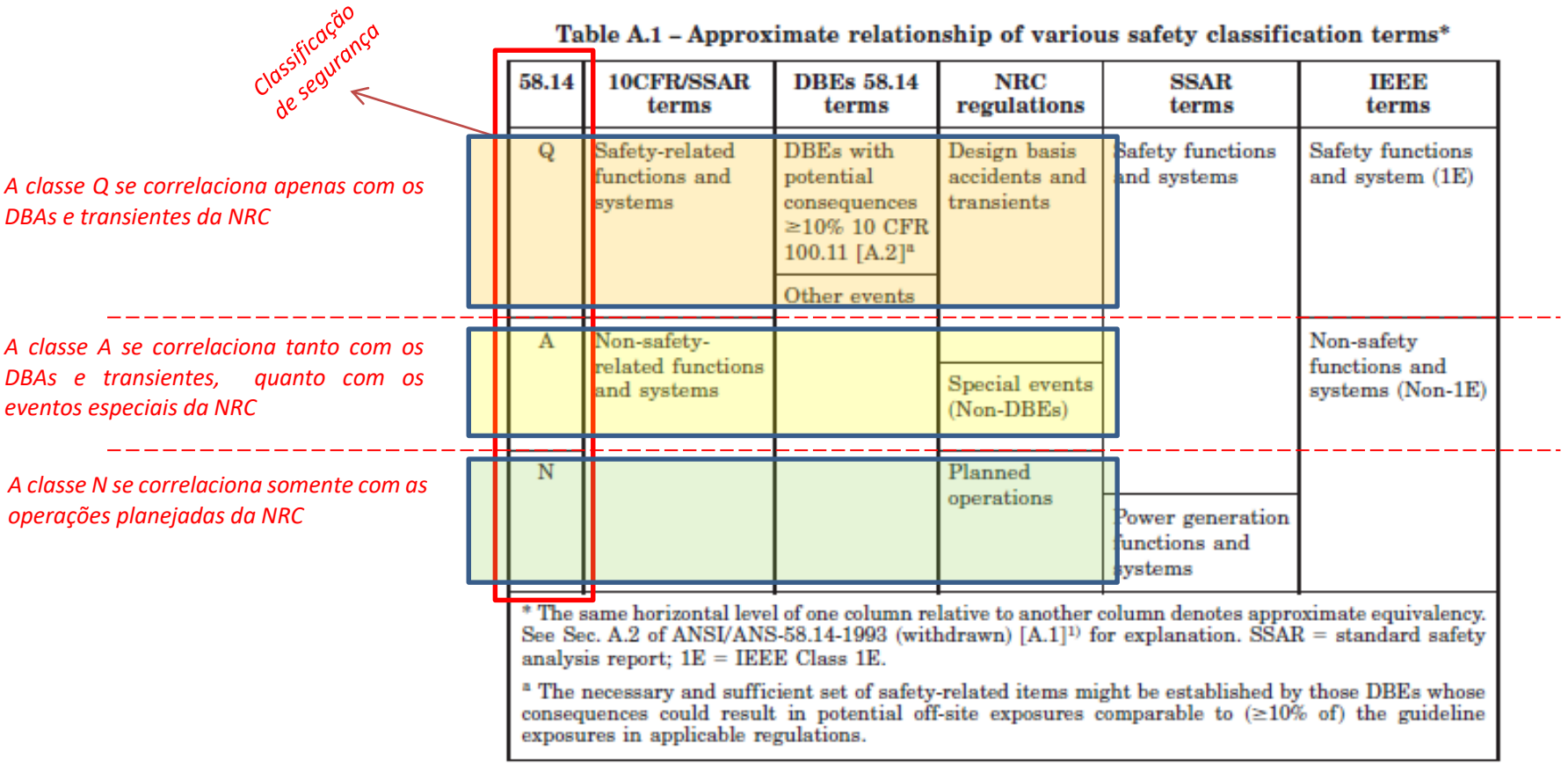


Table A.1 – Approximate relationship of various safety classification terms*

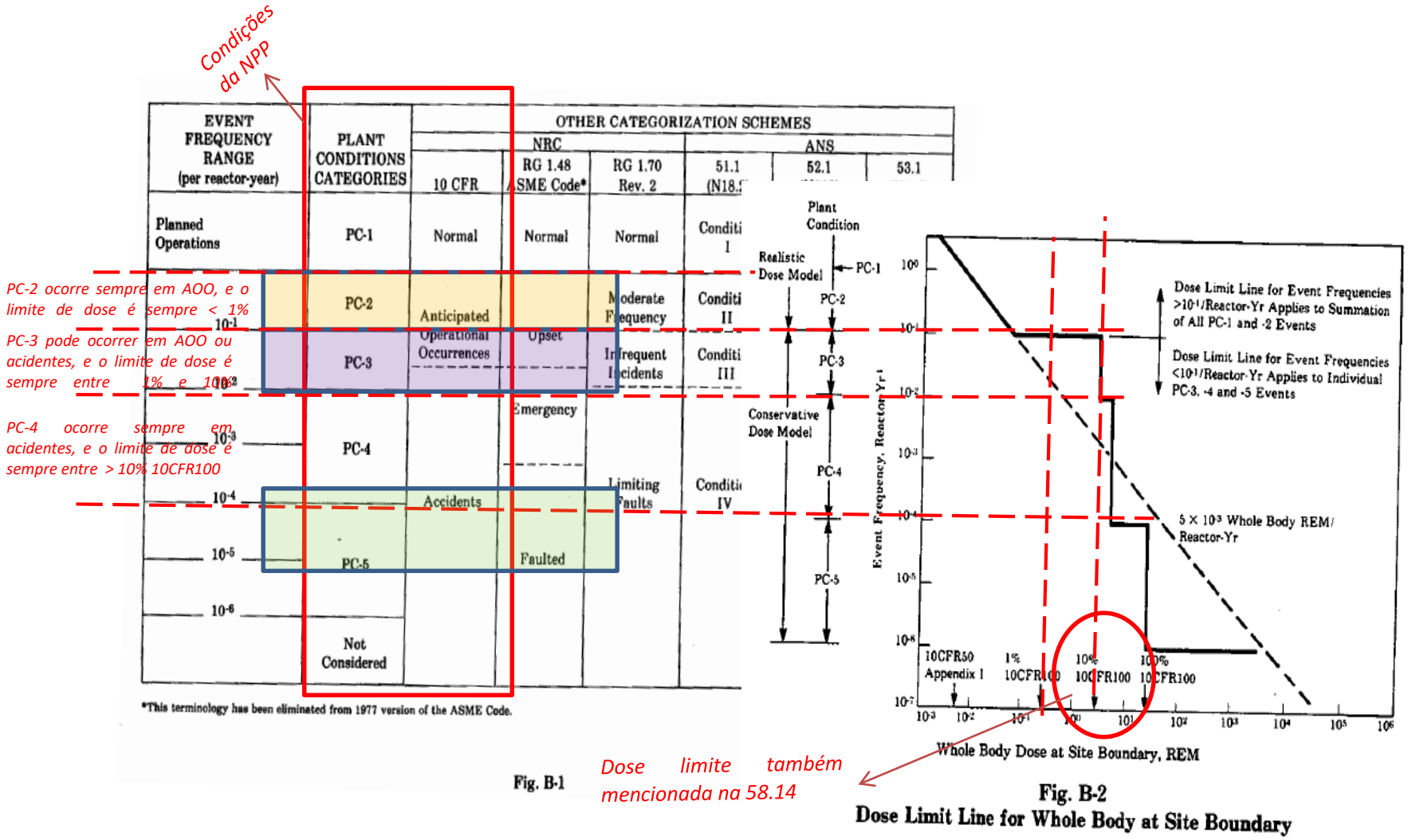
58.14	10CFR/SSAR terms	DBEs 58.14 terms	NRC regulations	SSAR terms	IEEE terms
Q	Safety-related functions and systems	DBEs with potential consequences ≥10% 10 CFR 100.11 [A.2][a]	Design basis accidents and transients	Safety functions and systems	Safety functions and system (1E)
		Other events			
A	Non-safety-related functions and systems				Non-safety functions and systems (Non-1E)
			Special events (Non-DBEs)		
N			Planned operations		
				Power generation functions and systems	

* The same horizontal level of one column relative to another column denotes approximate equivalency. See Sec. A.2 of ANSI/ANS-58.14-1993 (withdrawn) [A.1][1)] for explanation. SSAR = standard safety analysis report; 1E = IEEE Class 1E.

[a] The necessary and sufficient set of safety-related items might be established by those DBEs whose consequences could result in potential off-site exposures comparable to (≥10% of) the guideline exposures in applicable regulations.

Fonte: adaptado de ANSI/ANS 58.14 – Apêndice A

Figura 21 - Correlação - condições da planta e dose limite (ANSI/ANS 51.1)



Fonte: adaptado de ANSI/ANS 51.1 – Apêndice B.

ANEXO 4 – Modelos para as especificações dos Sistemas de I&C

1) CRITÉRIOS GERAIS DE I&C:

1.a) Critérios gerais de I&C – Especificação do Escopo Funcional

A tabela 10 tem como propósito a especificação do escopo funcional de I&C descrita no item 3.4.4.1. A sua concepção é em formato de matriz para permitir a aplicação dos diversos critérios (classe de segurança nuclear, meios de controle, objetivos de processo, sistemas de controle, condições da planta e categorias funcionais) à cada camada DiD definida pela NUREG-6303.

Tabela 10 – Exemplo de especificação do escopo funcional

Critérios Gerais de I&C - Definição de Escopo		Sistemas de controle e monitoramento Auxiliar	**Echelons of NUREG-6303**			
			Sistema de controle do Reator (SCR)	Sistema de SCRAM ou "*Reactor Trip*"	Sistema de Atuação de ESF	Sistema de Monitoramento e Indicação
Classe de Segurança Nuclear[iii]	FIS-N	X	-	-	-	-
	FIS-A	-	X	-	-	X
	FIS-Q	-	-	X	X	X
Meios de controle	Manual	X	ii	-	-	X
	Automático	X	X	X	X	-
	Monitoramento	X	-	-	-	X
Objetivos de segurança	Prevenção	-	X	-	-	X
	Proteção	-	-	X	X	X
	Mitigação	-	X	-	-	X
Sistemas de Processo	Sensores	X	X	X	X	X
	Atuadores	X	X	X	X	X
Sistemas de Controle	Módulos de ES com processo	X	X	X	X	-
	Solucionadores lógicos	X	X	X	X	-
	Indicadores	X	ii	-	-	X
	Alarmes	X	ii	-	-	X
	Acionadores manuais	X	ii	-	-	X

Critérios Gerais de I&C - Definição de Escopo		Sistemas de controle e monitoramento Auxiliar	**Echelons of NUREG-6303**			
			Sistema de controle do Reator (SCR)	Sistema de SCRAM ou "*Reactor Trip*"	Sistema de Atuação de ESF	Sistema de Monitoramento e Indicação
U.S.NRC Plant Conditions	Planned Operations	X	X	-	-	X
	Anticipated Operational Occurrences (AOO)	-	X	X	X	X
	Design basis accidents (DBE)[iv]	-	-	X	X	X
	Most significant DBEs[v]	-	-	X	X	X
	Special events (Non-DBEs)	-	X[i]	-	-	X
Categorias funcionais (Funções de Serviço "Ativas" de Nível 3)	Prover auxiliares do Primário e Secundário	X	-	-	-	-
	Controlar eventos externos (Agressões)	-	X	-	-	-
	Controlar a reatividade	-	X	-	-	-
	Controlar o resfriamento do núcleo	-	X	-	-	-
	Prover balanço massa e energia do primário	-	X	-	-	-
	Prover balanço massa e energia do secundário	-	X	-	-	-
	Prover balanço massa e energia da contenção	-	X	-	-	-
	Desligar o reator de modo diverso	-	X	-	-	X
	Iniciar o SCRAM e ESFAS	-	-	X	-	X
	Controlar o calor residual	-	-	-	X	X
	Acionar as ESF	-	-	-	X	X

Fonte: adaptado de NUREG-6303 e NUREG-7007.

Legenda de cores:

- Classificação nuclear indefinida (pelo projetista) X
- Não importante para a Segurança Nuclear X
- Importante para a Segurança Nuclear (A - ANSI 58.14) X
- Importante para a Segurança Nuclear (Q - ANSI 58.14) X

Notas:
i. Conforme NUREG/CR-6303: "Reactor control systems typically contain some equipment to satisfy the ATWS rule (10 CFR 50.62) or the requirement for a remote shutdown panel. Examples of such equipment include high-quality non-Class 1E equipment for which credit may be taken solely for compensating rare commonmode failures of Class 1E reactor protection equipment".
ii. Conforme NUREG/CR-6303: "Indicators, annunciators, and alarms may be included in the control echelon". Contudo, supõe-se neste trabalho, que tais componentes serão contemplados no escopo do "Monitoring and Information Echelon".
iii. De acordo com a ANSI/ANS-58.14 os SSCs classificados Q são classe 1E (IEEE-603) e os A classe N1E (com requisitos adicionais 1E da IEEE-603).
iv. De acordo com o apêndice C da ANSI/ANS 58.14 (item C.1.1) são DBEs: " typically include design basis transients".
v. De acordo com o apêndice C da ANSI/ANS 58.14 (item C.1.2) alguns exemplos são o LOCA e Ejeção de Barras de Controle.

1.b) Critérios gerais de I&C – Especificação dos Meios de Operação

A tabela 11 tem como propósito a especificação dos meios de operação descrita no item 3.4.4.2. A sua concepção é em formato de matriz para permitir a aplicação dos diversos meios de operação da UNM à cada camada DiD definida pela NUREG-6303, definindo inclusive o código identificador de cada meio.

Tabela 11 – Exemplo de especificação dos meios de Operação

Meios Disponíveis de Operação (MO#)			**Sistemas de Controle (SC#)**				
			Sistemas de controle e monitoramento Auxiliar	**Echelons of NUREG-6303**			
				Sistema de controle do Reator	Sistema de SCRAM ou "*Reactor Trip*"	Sistema de Atuação de ESF	Sistema de Monitoramento e Indicação
			SCA	SCR	SRT	ESF	SMI
Sala de Controle Principal	**Tela de Monitoramento Geral da UNM**	**Tco**	-	-	-	-	Tmo_SMI
	Consoles de Operação	**Cop**	Cop_SCA	-	-	-	Cop_SMI
	Console de Segurança & PAMS	**Cse**	-	-	-	-	Cse_SMI
Sala de Controle Remota	**Estações de controle**	**Etr**	Etr_SCA	-	-	-	Etr_SMI
	Painél de Shutdown & PAMS	**Psh**	-	Psh_SCR	-	-	-
Centro de Suporte Técnico	**Estações de trabalho**	**Etr**	Etr_SCA	-	-	-	-
Solucionadores Lógicos	**Controle remoto**	**Rem**	Rem_SCA	Rem_SCR	Rem_SRT	Rem_ESF	-
	Controle local	**Loc**	Loc_SCA	-	-	-	-
Interfaces de dados com o processo	**Módulo ES**	**Mes**	Mes _SCA	Mes _SCR	Mes _SRT	ii	ii

Fonte: adaptado de NUREG-6303 e NUREG-7007.

Notas:
i. As localizações descritas tomaram como referência o arranjo geral de uma UNM da tese de FREIRE (2018), com adaptações da AREVA (2016).
ii. Aconselha-se reduzir o número de interfaces com o campo, por se tratar de um projeto que visa otimização de volume e peso. Por esse motivo, os sinais podem ser compartilhados pelos sistemas com mesma classificação (uma interface do tipo N, outra do tipo A e outra do tipo Q).

A tabela 12 tem como propósito a apresentação do relatório constando em lista todos os meios de operação proposto na tabela 11.

Tabela 12 - Exemplo de relatório dos meios de operação

Subsistema de Controle		**Meios de I&C**		**Classificação Funcional**
Descrição	**Equipe**	**Cód.**	**Descrição**	
Sistema de Monitoramento e Controle (SMC)	ECUNM#1	Cop_SCA	Consoles de Operação do SCA	N
		Ecr_SCA	Estações de controle do SCA	N
		Etr_SCA	Estações de trabalho do SCA	N
		Rem_SCA	Controle remoto do SCA	N
		Mes _SCA	Módulo ES do SCA	N
		Psh_SCR	Painél de Shutdown & PAMS do SCR	A
		Rem_SCR	Controle remoto do SCR	A
		Tmo_SMI	Tela de Monitoramento Geral da UNM do SMI	A
		Cop_SMI	Consoles de Operação do SMI	A
		Ecr_SMI	Estações de controle do SMI	A
		Mes _SCR	Módulo ES do SCR	A
Sistema de Monitoramento e Proteção (SMP)	ECUNM#2	Cse_SMI	Console de Segurança & PAMS do SMI	Q
		Rem_SRT	Controle remoto do SRT	Q
		Rem_ESF	Controle remoto do ESF	Q
		Mes _SRT	Módulo ES do SRT	Q

1.c) Critérios gerais de I&C – Especificação do Plano Tecnológico

A tabela 13 tem como propósito a especificação do plano tecnológico para sensores de uma UNM seguindo o caminho descrito no item 3.4.4.3. Cada item da especificação é agrupada em três conjuntos: Escopo de uso, critérios de projeto e condições técnicas adicionais. Além disso, os itens da especificação podem ser direcionais para cada uma das cinco classificações adotadas, e em cada campo há uma explicação ou exemplos para a elaboração do plano tecnológico.

Tabela 13 - Exemplo de plano tecnológico para sensores

ESCOPO DE USO	**CLASSIFICAÇÃO FUNCIONAL (ANSI/ANS 58.14)**	Q (LOCA)	Q (non-LOCA)	A (LOCA)	A (non-LOCA)	N
	FLUIDO	Água desmineralizada, Água radioativa, Vapor, N2 etc.				
	ESTADO	Líquido, gás, vapor				
	POSIÇÃO DE MONTAGEM	Na tubulação, no equipamento, em suporte, na parede etc.				
	CLASSIFICAÇÃO DE INTEGRIDADE (ANSI/ANS 58.14)	C-1, C-2, C-3, ou NA		C-4 ou NA		NA
CRITÉRIOS DE PROJETO	**CLASSE ELÉTRICA (IEEE)**	1E		N1E		NA
	CATEGORIA SÍSMICA (ANSI/ANS 58.14)	I		II		NA
	AGRESSÕES	LOCA, Submersão, Radiação	Submersão, Radiação	LOCA, Submersão, Radiação	Submersão, Radiação	NA
	TIPO DE SENSORES	Temperatura: Pt100, termopar etc. / Vazão: Placa orifício, coriolis, ultrassônico etc. / Pressão: Dp cell, cristal piezo etc. / Nível: Dp cell, ultrassônico, radar etc.				
	SENSOR CARACT.	Simples, duplo etc.				
	OBSERVAÇÕES	Inserir performances ou acessórios (poços de medição, supressores de pressão, sifões, selo diafragma etc.)				
	DADOS TUBULAÇÃO/EQUIPAMENTO	Inserir dados de tubulação/equipamento: diâmetro nominal, espessura etc.				
INFORMAÇÕES TÉCNICAS ADICIONAIS	**DETALHES DO SENSOR**	Inserir classes de exatidão, números de fios condutores etc.				
	PROCESS RANGE	Inserir o range de medição do instrumento e respectiva incerteza.				
	MATERIAL BÁSICO	Inserir material básico de especificação do sensor.				
	MATERIAL DAS PARTES MOLHADAS	Inserir o material do sensor que tem contato com o fluido do processo (Aço inox 304, Alumínio, Bronze etc.)				
	MATERIAL DO INVÓLUCRO	Inserir o material do invólucro que protege o sensor e seus contatos elétricos de intempéries (Aço inox, aluminío, termoplástico etc.)				

	GRAU DE PROTEÇÃO	Inserir o grau de proteção IP e certificação INMETRO ou similar.
	CONEXÃO AO PROCESSO	Inserir especificação se é roscado, soldado etc., e os diâmetros (BSB, NPT etc.)
	CLASSE DE PRESSÃO	Especificar a classe de pressão do código industrial utilizado (ASME ou similar)
	CAPACIDADE DE CORRENTE ELÉTRICA DO CONTATO	Especificar a corrente de saída máxima do contato elétrico, e se é alternada ou contínua.
	TENSÃO DE ALIMENTAÇÃO	Especificar a tensão de suprimento elétrico necessário para alimentar o sensor (24Vcc, 120 Vac @60Hz, etc.)
	SINAL DE SAÍDA	Especificar o tipo de sinal de saída do sensor/transmissor (ôhmico, corrente, protocolo de rede) e o valor.
	CONEXÃO ELÉTRICA	Inserir especificação se é roscado, soldado etc., e os diâmetros (BSB, NPT etc.)
	FABRICANTE DE REF.	Inserir lista de fabricantes autorizados para fornecimento.

Fonte: adaptado de ANSI/ANS 51.1, ANSI/ANS 58.14, IAEA (1999 e 2008).

A tabela 14 tem como propósito a especificação do plano tecnológico para válvulas de controle (um tipo de atuador de processo) de uma UNM seguindo o caminho descrito no item 3.4.4.3. Cada item de especificação é disposto de forma análoga da tabela 13.

Tabela 14 - Exemplo de plano tecnológico para válvulas de controle

ESCOPO DE USO	**CLASSIFICAÇÃO FUNCIONAL (ANSI/ANS 58.14)**	Q (LOCA)	Q (non-LOCA)	A (LOCA)	A (non-LOCA)	N
	FLUIDO	Água desmineralizada, Água radioativa, Vapor, N2 etc.				
	ESTADO	Líquido, gás, vapor				
	POSIÇÃO DE MONTAGEM	Na tubulação, no equipamento, em suporte, na parede etc.				
	CLASSIFICAÇÃO DE INTEGRIDADE (ANSI/ANS 58.14)	C-1, C-2, C-3, ou NA				C-4 ou NA
CRITÉRIOS DE PROJETO	CLASSE ELÉTRICA (IEEE)	1E				N1E
	CATEGORIA SÍSMICA (ANSI/ANS 58.14)	I				II
	AGRESSÕES	LOCA, Submersão, Radiação	Submersão, Radiação	LOCA, Submersão, Radiação	Submersão, Radiação	NA
	TIPO DE VÁLVULA	Globo, Esfera, Gaveta etc.				
	TIPO ATUADOR	Motorizado, pneumático, hidráulico etc.				
	OBSERVAÇÕES	Inserir performances ou acessórios (volante, acumulador de energia etc.)				
	DADOS TUBULAÇÃO/EQUIPAMENTO	Inserir dados de tubulação/equipamento: diâmetro nominal, espessura etc.				
IN F O P	DETALHES DO ATUADOR	Inserir classes de exatidão, números de fios condutores etc.				

	PROCESS RANGE	Inserir o range do coeficiente de vazão, torque e respectivas incerteza.
	MATERIAL BÁSICO	Inserir material básico de especificação do corpo da válvula.
	MATERIAL DAS PARTES MOLHADAS	Inserir o material dos internos da válvula que tem contato com o fluido do processo (Aço inox 304, Alumínio, Bronze etc.)
	MATERIAL DO INVÓLUCRO	Inserir o material do invólucro que protege o atuador e seus contatos elétricos de intempéries (Aço inox, aluminío, termoplástico etc.)
	GRAU DE PROTEÇÃO	Inserir o grau de proteção IP do atuador e certificação INMETRO ou similar.
	CONEXÃO AO PROCESSO	Inserir especificação se a válvula é roscada, soldada etc., e os diâmetros (BSB, NPT etc.)
	CLASSE DE PRESSÃO	Especificar a classe de pressão do código industrial utilizado (ASME ou similar)
	CAPACIDADE DE CORRENTE ELÉTRICA DO CONTATO	Especificar a corrente de saída máxima do contato elétrico, e se é alternada ou contínua.
	TENSÃO DE ALIMENTAÇÃO	Especificar a tensão de suprimento elétrico necessário para alimentar o atuador (24Vcc, 120 Vac @60Hz, etc.)
	SINAL DE SAÍDA	Especificar o tipo de sinal de saída do atuador (tensão, corrente, protocolo de rede) e o valor.
	CONEXÃO ELÉTRICA	Inserir especificação se é roscado, soldado etc., e os diâmetros (BSB, NPT etc.)
	FABRICANTE DE REF.	Inserir lista de fabricantes autorizados para fornecimento.

Fonte: adaptado de ANSI/ANS 51.1, ANSI/ANS 58.14, IAEA (1999 e 2008).

A tabela 15 tem como propósito a especificação do plano tecnológico para módulos de controle de uma UNM seguindo o caminho descrito no item 3.4.4.3. Cada item de especificação é disposto de forma análoga da tabela 13.

Tabela 15 - Exemplo de plano tecnológico para módulos de controle

ESCOPO DE USO	**CLASSIFICAÇÃO FUNCIONAL (ANSI/ANS 58.14)**		Q (non-LOCA)	A (non-LOCA)	N
	FUNÇÃO DE CONTROLE		Safety-related	Non-safety related with augmented requirements	Non-safety related
CRITÉRIOS DE PROJETO	**CLASSE ELÉTRICA (IEEE)**		1E	N1E	NA
	CATEGORIA SÍSMICA (ANSI/ANS 58.14)		I	II	NA
	AGRESSÕES		Submersão, Radiação	Submersão, Radiação	NA
INFORMAÇÕES TÉCNICAS ADICIONAIS	**GERAL**	**FUNCÇÃO TÉCNICA**	Unidade de processamento, ou PLC de segurança	PLC	PLC, computador
		USO	Sistemas de alta confiabilidade	Sistemas de média confiabilidade	Sistemas de baixa confiabilidade
		RANGE TEMPERATURA	5ºC to 60ºC		

		SIL MÍNIMO	2	2	1
		ATENDIMENTO	IEC 61131-1 & IEC 61131-2	IEC 61131-1 & IEC 61131-2	IEC 61131-1 & IEC 61131-2
		DISPONIBILIDADE	Depende da malha de controle do processo		
		PRINCIPAIS CARACTERÍSTICAS	Falha segura	-	-
			Capacidade de redundância		
		PROTOCOLOS DE COMUNICAÇÃO	MPI, Profibus DP, Industrial Ethernet, Profinet and Profisafe		
		LINGUAGENS DE PROGR.	IEC 61508		
	MÓDULOS DE IO	**PROTOCOLOS DE COMUNICAÇÃO**	Profibus DP or Profinet		
		GRAU DE PROTEÇÃO	Inserir o grau de proteção IP do atuador e certificação INMETRO ou similar.		
	CARTÕES IO	**ENTRADA ANALÓGICA**	X	X	X
		SAÍDA ANALÓGICA	-	X	X
		ENTRADA DIGITAL	X	X	X
		SAÍDA DIGITAL	X	X	X
		RELÉ DIGITAL DE SÁIDA	X	-	-
		Other	Diagnóstico com alarmes		-
	ALIMENTAÇÃO ELÉTRICA	**PRINCIPAIS CARACTERÍSTICAS**	Diagnostics for Backplane voltages		
			Capacidade de redundância		-
		TENSÃO DE ENTRADA	Especificar a tensão de suprimento elétrico necessário para alimentar o atuador (24Vcc, 120 Vac @60Hz, etc.)		
		TENSÃO DE SAÍDA	Especificar o tipo de sinal de saída do atuador (tensão, corrente, protocolo de rede) e o valor.		
	FABRICANTE DE REF.		Inserir lista de fabricantes autorizados para fornecimento.		

Fonte: adaptado de ANSI/ANS 51.1, ANSI/ANS 58.14, IAEA (1999 e 2008).

2.a) Arquiteturas funcionais de I&C – Declinação funcional e classificação

A tabela 16 tem como propósito a declinação das funções de alto nível (do nível 1 ao 3) e suas respectivas classificação conforme o item 3.4.5.1. A sua concepção é em formato de tabela para permitir a declinação dos objetivo e funções de alto nível (níveis 1 e 2) para o nível 3, com suas devidas identificações, classificações e declinação dos pacotes de requisitos funcionais.

Tabela 16 - Exemplo declinação funcional de alto nível

Objetivos Gerais da UNM	**DISPONIBILIDADE**										**SEGURANÇA**[ii]			
Nível 1 (Objetivos da UNM)	**Gerar energia**										**Evitar ou mitigar vazamento radioativo**			
Nível 2 (Funções de Serviço)[i] (Baseada na 10CFR50.2 e GDC)	Auxiliar a operação da UNM		Gerenciar o material radioativo	Controlar as agressões	Gerar energia de fonte térmica nuclear						Ter capacidade de desligar o reator de forma segura		Evitar vazamentos radioativos	
Identificador FIS	FIS-N_1		FIS-A_1	FIS-A_2	FIS-A_3						FIS-Q_1		FIS-Q_2	
Pacote de Requisitos Funcionais[iii] (RFN)	RFN2-N_1 (Sem GDCs)		RFN2-A_1 (GDC: 60, 64, etc.)	RFN2-A_2 (GDC: 3, etc.)	RFN2-A_3 (GDC: 12, 13, 19, 34, 44, etc.)						RFN2-Q_1 (GDC: 12, 13, 15, 19, 20, 33, 34, 28, 29, 44, etc.)		RFN2-Q_2 (GDC: 13, 35, 38, 41, 56, 60, 64, etc.)	
Classificação de Segurança Nuclear (Baseada na ANSI/ANS 58.14)	[N] - NON-SAFETY-RELATED	[A] - NON-SAFETY-RELATED AUGMENTED REQUIREMENT									[Q] - SAFETY-RELATED			
Nível 3 (Funções de Serviço) (Baseado no U.S.NRC GDC e NUREG-0800)	Prover utilidades	Prover auxiliares do Primário e Secundário	Prover utilidades	Controlar eventos externos (Agressões)	Controlar a reatividade	Controlar o resfriamento do núcleo	Prover balanço massa e energia do primário	Prover balanço massa e energia do secundário	Prover balanço massa e energia da contenção	Desligar o reator de modo diverso	Prover utilidades	Executar o SCRAM e ESFAS	Controlar o calor residual	Executar ESF

Fonte: adaptado de 10CRF50, NUREG-0800 e ANSI/ANS 58.14.

Notas:
(i). A proposição das funções e requisitos GDC deste trabalho é apenas ilustrativa, conforme NUREG-0700 a análise funcional deve ser realizada por uma equipe multidisciplinar seguindo um programa complexo de interações. (ii) Assumiu-se neste item que a primeira das três funções básicas da 10CFR50.2 (Garantira a integridade da barreira de pressão do refrigerante do reator - RCPB) é puramente passiva, portanto foi desconsiderada desta análise. Destacam-se aqui apenas as funções ativas (controladas) da UNM.
*(iii). Nestes campos devem ser especificados os princípios de segurança nuclear ou GDCs (10CFR50 – app.A), e demais critérios gerais funcionais da UNM (requisitos funcionais de alto nível). O código "*RFN2-*N_1" identifica: Pacote de Requisitos Funcionais do Nível 2 para a Função Não-Importante para Segurança Nuclear #1.*

A tabela 17 tem como propósito a quebra (detalhamento) das funções de nível 3 em funções técnicas conforme o item 3.4.5.1. A sua concepção é em formato de matriz para permitir a relação de cada bloco de função de controle com as funções de nível 3. Esta relação define todas as funções técnicas de nível 3 necessárias, que serão a base para a declinação para os níveis inferiores (níveis 4 e 5), assim como determina os sistemas e equipes responsáveis.

Tabela 17 – Exemplo de declinação funcional e classificação

Classificação de Segurança Nuclear (Baseada na ANSI/ANS 58.14)			**[N] - NON-SAFETY-RELATED**		**[A] - NON-SAFETY-RELATED AUGMENTED REQUIREMENT**								**[Q] - SAFETY-RELATED**			
Nível 3 (Funções de Serviço)[i] (Baseado no U.S.NRC GDC e NUREG-0800)			Prover utilidades	Prover auxiliares do Primário e Secundário	Prover utilidades	Controlar eventos externos (Agressões)	Controlar a reatividade	Controlar o resfriamento do núcleo	Prover balanço massa e energia do primário	Prover balanço massa e energia do secundário	Prover balanço massa e energia da contenção	Desligar o reator de modo diverso	Prover utilidades	Executar o SCRAM e ESFAS	Controlar o calor residual	Executar ESF
Funções técnicas de I&C (Nível 3)			FIS-N_1.1	FIS-N_1.2	FIS-A_1.1	FIS-A_2.1	FIS-A_3.1	FIS-A_3.2	FIS-A_3.3	FIS-A_3.4	FIS-A_3.5	FIS-A_3.6	FIS-Q_1.1	FIS-Q_1.2	FIS-Q_1.2	FIS-Q_2.1
Equipe	**Subsistema (Nível 3)**	**Requisitos Funcionais**[iii] (RFN)	RFN3-N_1.1	RFN3-N_1.2	RFN3-A_1.1	RFN3-A_2.1	RFN3-A_3.1	RFN3-A_3.2	RFN3-A_3.3	RFN3-A_3.4	RFN3-A_3.5	RFN3-A_3.6	RFN3-Q_1.1	RFN3-Q_1.2	RFN3-Q_1.2	RFN3-Q_2.1
EPUNM #1	**Sistema de Barras de Controle** (Baseado no item 4.2 da ANSI/ANS 51.1)	Medir o processo					#1							#1		
		Manipular o processo					#2							#2		
		Trocar dados de I&C com processo					#3							#3		
		Solucionar as lógicas de controle					#4									
		Indicar as variáveis de processo e controle					#5									
		Gerar alarmes de processo e controle					#6									
		Manipular o processo manualmente					#7									
EPUNM #2	**Sistema do Primário** (Baseado no item 4.4, 4.5 e 4.6 da ANSI/ANS 51.1)	Medir o processo		#1			#8	#1						#4	#1	#1
		Manipular o processo		#2			#9	#2						#5	#2	#2
		Trocar dados de I&C com processo														
		Solucionar as lógicas de controle														
		Indicar as variáveis de processo e controle														
		Gerar alarmes de processo e controle														

		Manipular o processo manualmente															
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
EPUNM #3	**Sistema de Utilidades e Controle de Agressões** (Baseado no item 4.12, 4.13, 4.14, 4.15 e parte da 4.16 da ANSI/ANS 51.1)	Medir o processo	#1		#1	#1							#1				
		Manipular o processo	#2		#2	#2							#2				
		Trocar dados de I&C com processo	#3		#3	#3							#3				
		Solucionar as lógicas de controle	#4		#4	#4							#4				
		Indicar as variáveis de processo e controle	#5		#5	#5							#5				
		Gerar alarmes de processo e controle	#6		#6	#6							#6				
		Manipular o processo manualmente	#7		#7	#7							#7				
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
ECUNM #1	**Sistema de Controle Normal** (Baseado no item 4.2 da ANSI/ANS 51.1)	Medir o processo															
		Manipular o processo															
		Trocar dados de I&C com processo		#3			#10	#3	#1	#1	#1	#1					
		Solucionar as lógicas de controle		#4			#11	#4	#2	#2	#2	#2					
		Indicar as variáveis de processo e controle	#8	#5	#8	#8	#12	#5	#3	#3	#3	#3	#8				
		Gerar alarmes de processo e controle	#9	#6	#9	#9	#13	#6	#4	#4	#4	#4	#9				
		Manipular o processo manualmente		#7			#14	#7	#5	#5	#5	#5					
ECUNM #2	**Sistema de Controle de Segurança** (Baseado no item 4.2 da ANSI/ANS 51.1)	Medir o processo															
		Manipular o processo															
		Trocar dados de I&C com processo												#6	#3	#3	
		Solucionar as lógicas de controle												#7	#4	#4	
		Indicar as variáveis de processo e controle												#8	#5	#5	
		Gerar alarmes de processo e controle												#9	#6	#6	
		Manipular o processo manualmente												#10	#7	#7	

Fonte: adaptado de 10CRF50, NUREG-0800 e ANSI/ANS 58.14.

Notas:
(i). A proposição das funções deste trabalho é apenas ilustrativa, conforme NUREG-0700 a análise funcional deve ser realizada por uma equipe multidisciplinar seguindo um programa complexo de interações.
(ii). A tabela é apenas ilustrativa. Para simplificar, buscou-se colocar o símbolo "(...)"para indicar que podem haver n itens a serem especificados para atender um projeto específico.
*(iii). Nestes campos devem ser especificados os princípios de segurança nuclear ou GDCs (10CFR50 – app.A), e demais critérios gerais funcionais da UNM (requisitos funcionais de alto nível). O código "*RFN3-*N_1.1" identifica: Pacote de Requisitos Funcionais do Nível 3 para a Função Não-Importante para Segurança Nuclear #1.1.*

Cada uma das funções técnicas relacionadas na tabela 17 é baseada na tabela 18, onde são especificados o tipo, a camada de automação e o código a ser utilizado nos relatórios.

Tabela 18 – Exemplo de tabela base com categorias funcionais

Categorias de Funções Técnicas de I&C - FTC			
Descrição	**Tipo**	**Camada**	**Cód.**
Medir o processo	SENSOR	0	S
Manipular o processo	ATUADOR	0	A
Trocar dados de I&C com processo	MODULO_IO	1	MIO
Solucionar as lógicas de controle	CONTROLADOR	2	CTR
Indicar as variáveis de processo e controle	INDICADOR	3	HSI
Gerar alarmes de processo e controle	ALARME	3	HSI
Manipular o processo manualmente	BOTOEIRA	3	HSI

A tabela 19 lista o resultado das combinações da tabela 17 em formato de relatório, utilizando os dados da tabela 18.

Tabela 19 – Exemplo de Relatório dos Blocos de Função

Equipe	**Subsistema**		**Função de Serviço - FS# (FIS# + SS#)**		**Função de Técnica (FS# + SS#)**		**Bloco de Controle (Cod.FTC + FT#)**	**Camada de I&C**	**Grupo**
EPUNM #1	SS#1	Sistema de Barras de Controle	FIS-A_3.1.1	Controlar a reatividade	FIS-A_3.1.1#1	Medir o processo para Controlar a reatividade	S_FIS-A_3.1.1#1	0	S_FIS-A
EPUNM #1	SS#1	Sistema de Barras de Controle	FIS-A_3.1.1	Controlar a reatividade	FIS-A_3.1.1#2	Manipular o processo para Controlar a reatividade	A_FIS-A_3.1.1#2	0	A_FIS-A
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

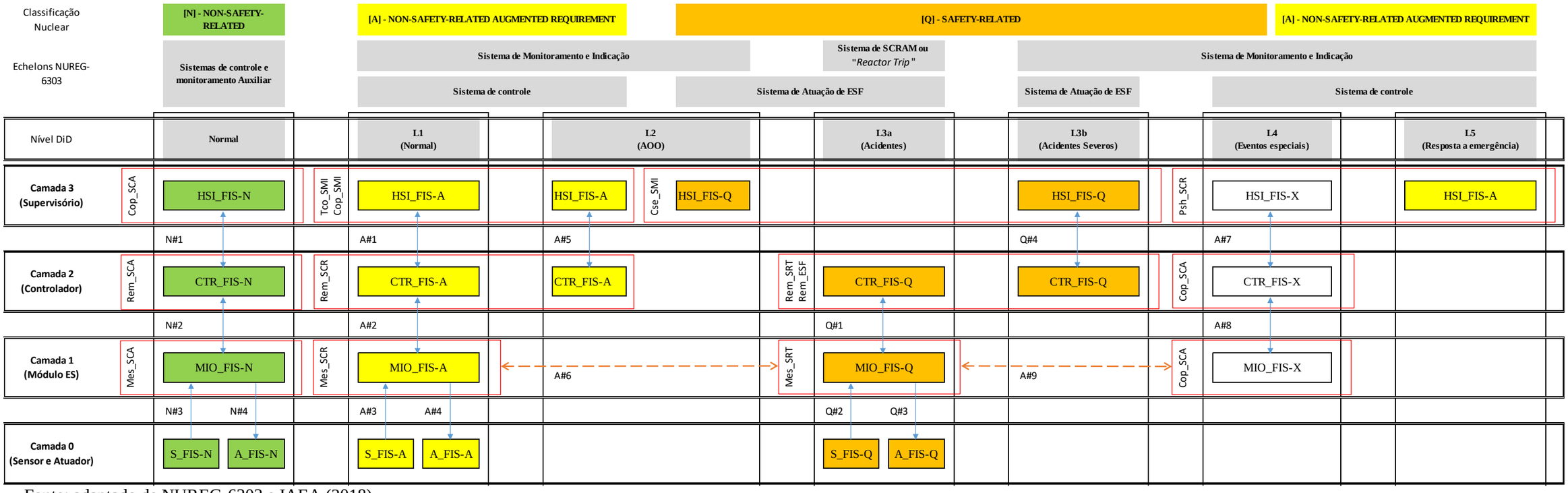
Equipe	Subsistema		Função de Serviço - FS# (FIS# + SS#)		Função de Técnica (FS# + SS#)		Bloco de Controle (Cod.FTC + FT#)	Camada de I&C	Grupo
EPUNM #2	SS#2	Sistema do Primário	FIS-N_1.2.2	Prover auxiliares do Primário e Secundário	FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	0	S_FIS-N
EPUNM #2	SS#2	Sistema do Primário	FIS-N_1.2.2	Prover auxiliares do Primário e Secundário	FIS-N_1.2.2#2	Manipular o processo para Prover auxiliares do Primário e Secundário	A_FIS-N_1.2.2#2	0	A_FIS-N
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
ECUNM #1	SS#4	Sistema de Controle	FIS-N_1.1.4	Prover utilidades	FIS-N_1.1.4#8	Indicar as variáveis de processo e controle para Prover utilidades	HSI_FIS-N_1.1.4#8	3	HSI_FIS-N
ECUNM #1	SS#4	Sistema de Controle	FIS-N_1.1.4	Prover utilidades	FIS-N_1.1.4#9	Gerar alarmes de processo e controle para Prover utilidades	HSI_FIS-N_1.1.4#9	3	HSI_FIS-N
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
ECUNM #2	SS#5	Sistema de Controle de Segurança	FIS-Q_1.2.5	Executar o SCRAM e ESFAS	FIS-Q_1.2.5#6	Trocar dados de I&C com processo para Executar o SCRAM e ESFAS	MIO_FIS-Q_1.2.5#6	1	MIO_FIS-Q
ECUNM #2	SS#5	Sistema de Controle de Segurança	FIS-Q_1.2.5	Executar o SCRAM e ESFAS	FIS-Q_1.2.5#7	Solucionar as lógicas de controle para Executar o SCRAM e ESFAS	CTR_FIS-Q_1.2.5#7	2	CTR_FIS-Q

Notas:
(i). A tabela é apenas ilustrativa. Para simplificar, buscou-se colocar o símbolo "(...)"para indicar que podem haver n itens a serem especificados para atender um projeto específico.

2.b) Arquiteturas funcionais de I&C – Especificação das Interfaces Funcionais e Condições da Planta

A tabela 20 tem como propósito a especificação das interfaces entre os blocos de função e sua alocação a cada condição da planta conforme proposto no item 3.4.5.2. A sua concepção é em formato de matriz para permitir a alocação de cada bloco de função de controle em cada camada de automação (verticalmente) e em cada nível DiD (horizontalmente). Após a alocação, são delimitados a cada bloco de função o meio de controle responsável e determinadas todas as necessidades de interfaces entre os blocos de função.

Tabela 20 - Exemplo de especificação de interfaces funcionais e condições da UNM



Fonte: adaptado de NUREG-6303 e IAEA (2018).

Na tabela 21 é apresentado o relatório que é uma lista resultada do diagrama definido na tabela 20. Neste relatório são listados os meios de origem e destino para cada interface funcional.

Tabela 21 - Exemplo de resultado das interfaces

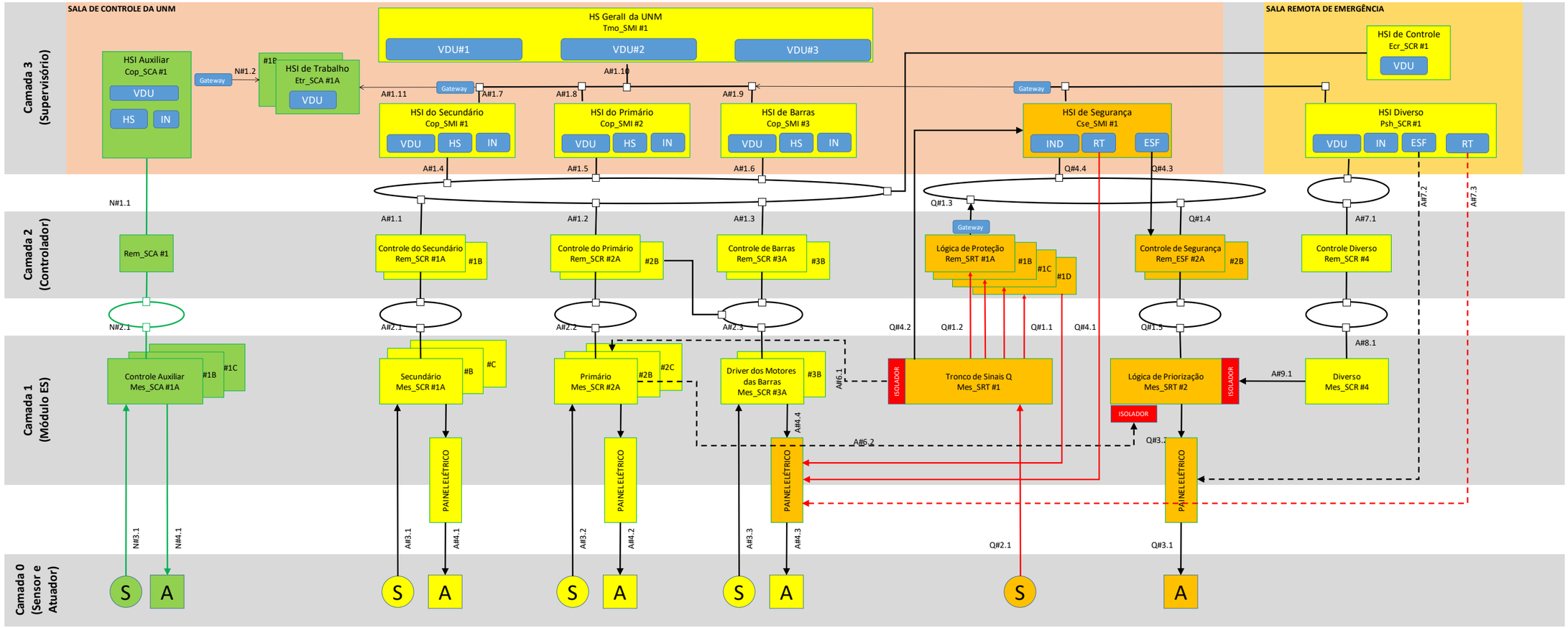
Interface	ORIGEM			DESTINO			DiD
	Gr. FTC	MEIO I&C	Descrição	Gr. FTC	MEIO I&C	Descrição	
N#1	CTR_FIS-N	Rem_SCA	Controle remoto do SCA	HSI_FIS-N	Cop_SCA	Consoles de Operação do SCA	NA
N#2	CTR_FIS-N	Rem_SCA	Controle remoto do SCA	MIO_FIS-N	Mes_SCA	Módulo ES do SCA	NA
N#3	S_FIS-N	SS#1	Sistema de Controle de Barra	MIO_FIS-N	Mes_SCA	Módulo ES do SCA	NA
N#4	A_FIS-N	SS#1	Sistema de Controle de Barra	MIO_FIS-N	Mes_SCA	Módulo ES do SCA	NA
A#1	CTR_FIS-A	Rem_SCR	Controle remoto do SCR	HSI_FIS-A	Cop_SMI	Consoles de Operação do SMI	1
A#2	CTR_FIS-A	Rem_SCA	Controle remoto do SCA	MIO_FIS-A	Mes_SCR	Módulo ES do SCR	1
A#3	S_FIS-A	SS#1	Sistema de Controle de Barra	MIO_FIS-A	Mes_SCR	Módulo ES do SCR	1
A#4	A_FIS-A	SS#1	Sistema de Controle de Barra	A_FIS-A	SS#1	Sistema de Controle de Barra	1
A#5	CTR_FIS-A	Rem_SCR	Controle remoto do SCR	HSI_FIS-A	Cop_SMI	Consoles de Operação do SMI	2
A#6	MIO_FIS-A	Mes_SCR	Módulo ES do SCR	MIO_FIS-Q	Mes_SRT	Módulo ES do SRT	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Notas:(i). A tabela é apenas ilustrativa. Para simplificar, buscou-se colocar o símbolo "(...)"para indicar que há n itens a serem especificados para atender um projeto específico.

2.c) Arquiteturas funcionais de I&C – Especificação da Arquitetura Global e Interfaces

Na figura 22 é apresentada arquitetura global e as interfaces conforme proposto no item 3.4.5.3. Na arquitetura, cada meio de controle definido na tabela 20 é distribuída em suas camadas de automação, dispondo os grupos da esquerda para a direita de acordo com a estratégia DiD.

Figura 22 - Exemplo de especificação de arquitetura global e interfaces



Fonte: adaptado de IAEA (2018) e AREVA (2007).

Notas:
(i). O propósito deste modelo não é esgotar as possibilidades funcionais, mas somente apresentar um esboço para facilitar o entendimento do declínio das interfaces de dados.

3) ARQUITETURAS TÍPICAS DE I&C E RELATÓRIOS ES E FC

3.a) Arquitetura típica e relatório ES - Especificação das Malhas de Controle

A tabela 22 especifica as necessidades de controle e monitoramento (C&M) para cada fase de estados dos sistemas, conforme item 3.4.6.1. Os passos para esta definição devem ser: primeiro identificar as necessidades de interfaces para o operador (HSI) e as necessidades de processamentos de controle (sistemas de controle). O segundo passo é definir se as HSIs e/ou controles deverão ser implementados remotamente ou localmente.

Legenda:

Necessidades de HSI:

- = Não aplicável;
C = Comando iniciador do controle;
M = Monitoramento; e
C&M = Comando e monitoramento.

Necessidades de Controle:

- = Não aplicável; e
X = Necessário.

Tabela 22 - Exemplo de especificação de malhas de controle (necessidades)

SS	Fase	Grupo FTC	Estado origem	Estado destino	Necessidades de HSI		Necessidades de Controle	
					Remoto	Local	Remoto	local
1.1	F1	CTR_FIS-Q	POTÊNCIA	SCRAM	C&M	C&M	X	X
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
2.1	F1	CTR_FIS-A	DEGRADADO	RESFRIANDO	-&M	C&-	X	X
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
3.1	F1	CTR_FIS-N	DESLIGADO	OPERANDO	C&M	-	X	-
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
4.1	F1	CTR_FIS-N	DESLIGADO	NOMINAL	-	C&M	-	X
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

A tabela 23 detalha o controle e monitoramento (C&M) para cada fase de estados dos sistemas, conforme item 3.4.6.1. Os passos para esta definição deve ser o detalhamento das necessidades levantadas anteriormente, especificando se as ações dos comandos são manuais, semiautomáticas ou automáticas, se as ações de controle são lógicas de intertravamento, regulagem, proteção ou só monitoramento.

Legenda:

Níveis de HSI (C&M):

Opções de comando:
- = Não aplicável;
M = Manual;
S = Semi automático.

Opções de Monitoramento:
- = Não aplicável; e
Indicação = I;
Alarme (Visual = V; Sonoro = S; Ambos = A).

Níveis de automação (C):

Opções de ações de comando:
- = Não aplicável;
I = Intertravamento (*on-off*);
R = Regulagem (contínua);

P = Intertravamento de proteção.

Tabela 23 - Exemplo de especificação de malhas de controle (Meios)

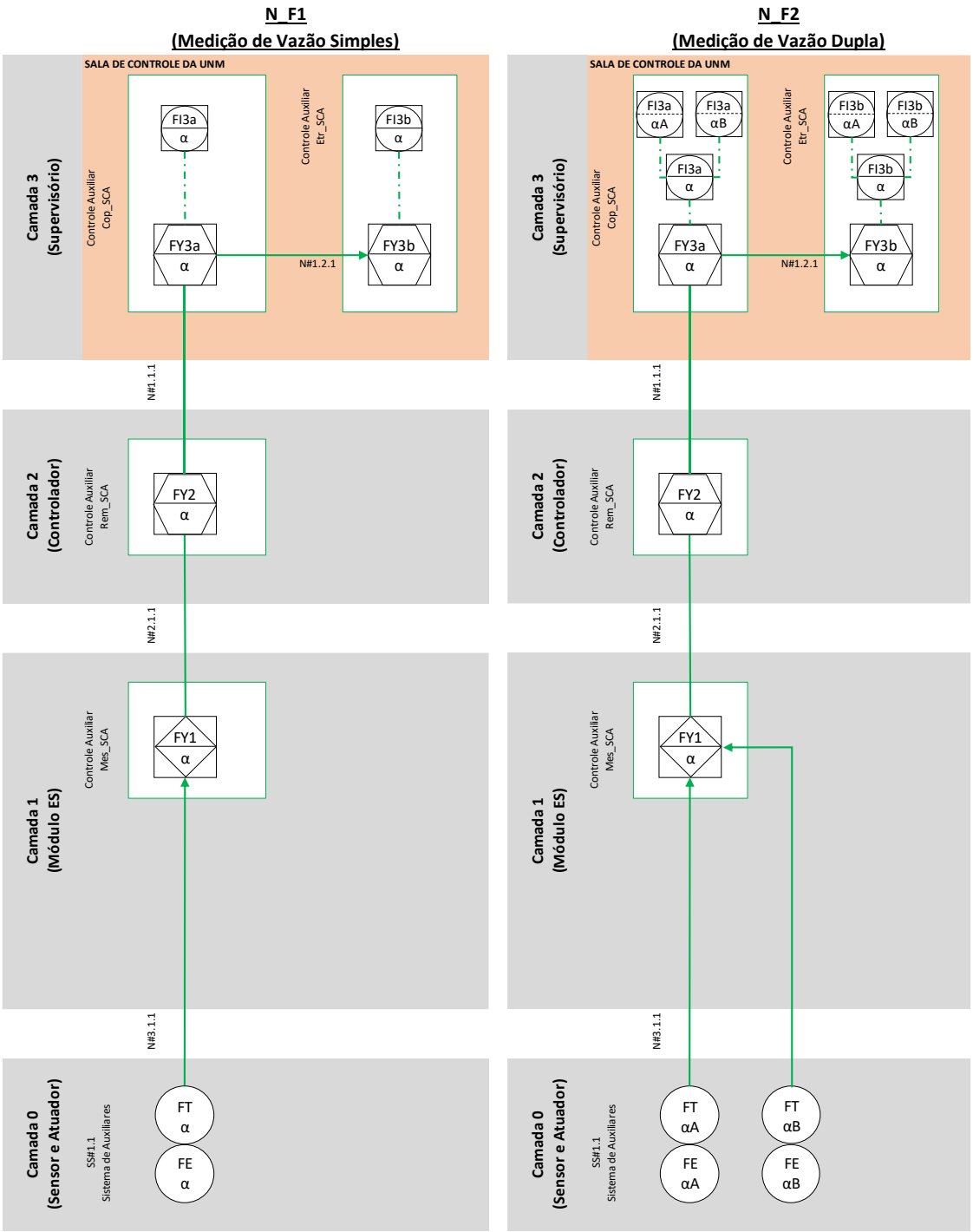
Sub-Sistema Nível 4	Estado/Fase	Função de Controle	BFT#	Atuadores e Sensores	Parâmetro ou Evento	Ação de Controle	Meios de HSI (interfaces providas para o operador)										Meios de Controle (interfaces provida por sistemas de controle)							
							Remoto Normal			Remoto Normal e Preventivo			Remoto Proteção	Remoto Mitigação		Local	Remoto Normal	Remoto Normal e Preventivo			Remoto Proteção		Remoto Mitigação	Local
							Auxiliar	Trabalho	Geral	Secundário	Primário	Barras	Segurança	Controle Diverso	Control Diverso		Auxiliar	Secundário	Primário	Barras	Proteção	Controle	Control Diverso	
							Cop_SCA #1	Etr_SCA #1	Tmo_SMI #1	Cop_SMI #1	Cop_SMI #2	Cop_SMI #3	Cse_SMI #1	Ecr_SCR #1	Psh_SCR #1		Rem_SCA #1	Rem_SCR #1	Rem_SCR #2	Rem_SCR #3	Rem_SRT #1	Rem_ESF #1	Rem_SCR #4	
SS#1.1	F1	SCRAM#1	A_FIS-Q_1.2.1#2	A_FIS-Q_XXX (Painel RT) S_FIS-Q_XXX (Sensores Prot.)	RT signal (2oo4)	Desalimentar o Painel RT	-	-	-	-	-	-	M&I	-	M&I	-	-	-	-	-	P	-	-	-
SS#1.1	SCRAM	SCRAM#2	HSI_FIS-A_3.1.1#5	A_FIS-Q_XXX (Painel RT) S_FIS-Q_XXX (Sensores Prot.)	(if) F1 executado	Estado do SS#1.1 vai para “SCRAM”	-	-	-	-	-	-	-	-	-	-&I	-	-	-	-	-	-	-	I
SS#4.1	SCRAM	SCRAM#3	HSI_FIS-A_3.2.4#5	A_FIS-Q_XXX (Painel RT) S_FIS-Q_XXX (Sensores Prot.)	(if) F1_SS#1.1 executado	Estado do SS#1.1 vai para “SCRAM”	-	-	-&I	-&I	-&I	-&I	-	-&I	-&I	-	-	-	-	I	-	-	-	-
SS#2.1	F1	TROCA BOMBA	A_FIS-A_3.2.2#2	A_FIS-A_XXX (Bomba Prim) S_FIS-Q_XXX (Sensores Prim)	(if) bomba principal = “fail” (and) bomba reserve disponível	Ligar Bomba Reserva	-	-	-	-	S&V	-	-	S&V	-	M&A	-	-	-	P	-	-	-	-	-
SS#4.1	RESFRIANDO	CIRCULAR REFREIGERANTE	HSI_FIS-A_3.2.4#5	A_FIS-A_XXX (Bomba Prim) S_FIS-Q_XXX (Sensores Prim)	(if) F1_SS#2.1 executado	Estado do SS#2.1 vai para “RESFRIANDO” (and) Controlar Primário	-	-	-&I	-	-&I	-	-	-&I	-	-	-	-	-	R	-	-	-	-

Sub-Sistema Nível 4	Estado/Fase	Função de Controle	BFT#	Atuadores e Sensores	Parâmetro ou Evento	Ação de Controle	Meios de HSI (interfaces providas para o operador)										Meios de Controle (interfaces provida por sistemas de controle)							
							Remoto Normal			Remoto Normal e Preventivo			Remoto Proteção	Remoto Mitigação		Local	Remoto Normal	Remoto Normal e Preventivo			Remoto Proteção		Remoto Mitigação	Local
							Auxiliar	Trabalho	Geral	Secundário	Primário	Barras	Segurança	Controle Diverso	Control Diverso		Auxiliar	Secundário	Primário	Barras	Proteção	Controle	Control Diverso	
							Cop_SCA #1	Etr_SCA #1	Tmo_SMI #1	Cop_SMI #1	Cop_SMI #2	Cop_SMI #3	Cse_SMI #1	Ecr_SCR #1	Psh_SCR #1		Rem_SCA #1	Rem_SCR #1	Rem_SCR #2	Rem_SCR #3	Rem_SRT #1	Rem_ESF #1	Rem_SCR #4	
SS#3.1	F1	CONTROLAR VAZÃO#1	HSI_FIS-N_1.2.4#5	A_FIS-N_XXX (ex. Válvula) S_FIS-N_XXX (Sensores)	Alimentadores #1 (and) #2 ligados	Alimentar válvulas de controle #1, #2 etc.	-	-	-	-	-	-	-	-	-	M&I	-	-	-	-	-	-	-	-
SS#3.1	OPERANDO	CONTROLAR VAZÃO#2	HSI_FIS-N_1.2.4#5	A_FIS-N_XXX (ex. Válvula) S_FIS-N_XXX (Sensores)	(if) F1_SS#4.1 executado	Estado do SS#4.1 vai para “NOMINAL”	-&I	-&I	-&I	-	-	-	-	-	-	M&I	R	-	-	-	-	-	-	-
SS#4.1	F1	LIGANDO SCR	HSI_FIS-N_1.2.4#5	Rem_SCR#1, 2, 3 Mes_SCR#1, 2, 3	Alimentadores #1 (and) #2 (and) #3 ligados	Ligar Gabinetes de controle	-	-	-	-	-	-	-	-	-	S&I	-	-	-	-	-	-	-	I
SS#4.1	NOMINAL	LIGANDO SCR	HSI_FIS-N_1.2.4#5	Rem_SCR#1, 2, 3 Mes_SCR#1, 2, 3	(if) F1_SS#4.1 executado	Estado do SS#4.1 vai para “NOMINAL”	-&I	-&I	-&I	-	-	-	-	-&I	-	-	I	-	-	-	-	-	-	-

3.b) Arquitetura típica e relatório ES - Especificação das Arquiteturas Típicas

Na figura 23 são apresentados exemplos de arquiteturas típicas para sensores conforme descrito no item 3.4.6.2.

Figura 23 - Exemplo de especificação de arquiteturas típicas para sensores



Fonte: Adaptado da simbologia e abreviações ISA 5.1.

Na tabela 24 são apresentadas as especificações de cada interface de dados e blocos de função apresentadas na figura 23.

Tabela 24 - Exemplo de especificação de interfaces típicas para sensores

N_F1
(Medição de Vazão Simples)

Interfaces de Dados

MALHA	LINK	TIPO	PROTOCOLO	DE	PARA
F-α	N#1.1.1	Digital	Ethernet	SS#4.1_FY2-α	SS#4.1_FY3a-α
F-α	N#1.2.1	Digital	Ethernet	SS#4.1_FY3a-α	SS#4.1_FY3b-α
F-α	N#2.1.1	Digital	Ethernet	SS#4.1_FY1-α	SS#4.1_FY2-α
F-α	N#3.1.1	Analógico	4-20mA + HART	SS#1.1_FT-α	SS#4.1_FY1-α

Camada 0 (Sensor e Atuador)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#1.1_FE-α	S_FIS-N	S_FIS-N_1.2.2#1	Sensor de vazão
F-α	SS#1.1_FT-α	S_FIS-N	S_FIS-N_1.2.2#1	Transmissor de pressão diferencial

Camada 1 (Módulo ES)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY1-α	MIO_FIS-N	MIO_FIS-N_1.2.4#3	Cartão de entrada e saída

Camada 2 (Controlador)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY2-α	CNTR_FIS-N	CTR_FIS-N_1.2.4#4	Programador Lógico - PLC

Camada 3 (Supervisório)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	PC industrial
F-α	SS#4.1_FI3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	Indicação virtual em Tela LCD - Vazão
F-α	SS#4.1_FY3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	PC industrial
F-α	SS#4.1_FI3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	Indicação virtual em PC - Vazão

N_F2
(Medição de Vazão Dupla)

Interfaces de Dados

MALHA	LINK	TIPO	PROTOCOLO	DE	PARA
F-α	N#1.1.1	Digital	Ethernet	SS#4.1_FY2-α	SS#4.1_FY3a-α
F-α	N#1.2.1	Digital	Ethernet	SS#4.1_FY3a-α	SS#4.1_FY3b-α
F-α	N#2.1.1	Digital	Ethernet	SS#4.1_FY1-α	SS#4.1_FY2-α
F-α	N#3.1.1	Analógico	4-20mA + HART	SS#1.1_FT-αA	SS#4.1_FY1-α
F-α	N#3.1.1	Analógico	4-20mA + HART	SS#1.1_FT-αB	SS#4.1_FY1-α

Camada 0 (Sensor e Atuador)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#1.1_FE-αA	S_FIS-N	S_FIS-N_1.2.2#1	Sensor de vazão
F-α	SS#1.1_FT-αA	S_FIS-N	S_FIS-N_1.2.2#1	Transmissor de pressão diferencial
F-α	SS#1.1_FE-αB	S_FIS-N	S_FIS-N_1.2.2#1	Sensor de vazão
F-α	SS#1.1_FT-αB	S_FIS-N	S_FIS-N_1.2.2#1	Transmissor de pressão diferencial

Camada 1 (Módulo ES)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY1-α	MIO_FIS-N	MIO_FIS-N_1.2.4#3	Cartão de entrada e saída

Camada 2 (Controlador)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY2-α	CNTR_FIS-N	CTR_FIS-N_1.2.4#4	Programador Lógico - PLC

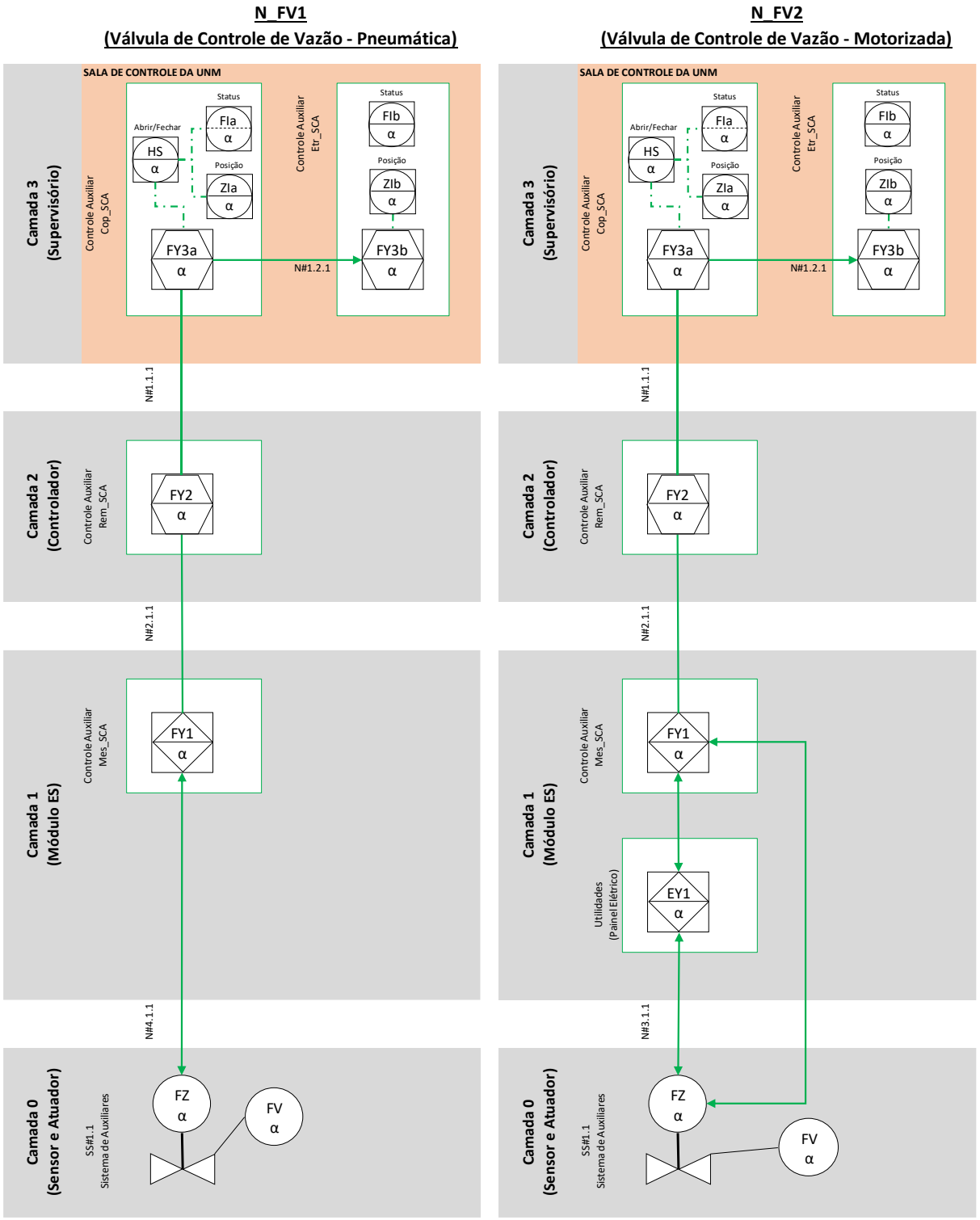
Camada 3 (Supervisório)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	PC industrial
F-α	SS#4.1_FI3a-α	HSI_FIS-N	NA	Indicação virtual em Tela LCD - Síntese vazão
F-α	SS#4.1_FI3a-αA	HSI_FIS-N	NA	Indicação oculta em Tela LCD - Vazão
F-α	SS#4.1_FI3a-αB	HSI_FIS-N	NA	Indicação oculta em Tela LCD - Vazão
F-α	SS#4.1_FY3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	PC industrial
F-α	SS#4.1_FI3b-α	HSI_FIS-N	NA	Indicação virtual em PC - Vazão
F-α	SS#4.1_FI3b-αA	HSI_FIS-N	NA	Indicação virtual em PC - Vazão
F-α	SS#4.1_FI3b-αB	HSI_FIS-N	NA	Indicação virtual em PC - Vazão

Fonte: Adaptado das abreviações ISA 5.1.

Na figura 24 são apresentados exemplos de arquiteturas típicas para atuadores conforme descrito no item 3.4.6.2.

Figura 24 - Exemplo de especificação de arquiteturas típicas para atuadores



Fonte: Adaptado da simbologia e abreviações ISA 5.1.

Na tabela 25 são apresentadas as especificações de cada interface de dados e blocos de função apresentadas na figura 24.

Tabela 25 - Exemplo de especificação de interfaces típicas para atuadores

N_FV1
(Válvula de Controle de Vazão - Pneumática)

Interfaces de Dados

MALHA	LINK	TIPO	PROTOCOLO	DE	PARA
F-α	N#1.1.1	Digital	Ethernet	SS#4.1_FY2-α	SS#4.1_FY3a-α
F-α	N#1.2.1	Digital	Ethernet	SS#4.1_FY3a-α	SS#4.1_FY3b-α
F-α	N#2.1.1	Digital	Ethernet	SS#1.1_FZ-α	SS#4.1_FY2-α
F-α	N#4.1.1a	Analógico	4-20mA + HART	SS#4.1_FY1-α	SS#1.1_FZ-α
F-α	N#4.1.1b	Analógico	4-20mA + HART	SS#1.1_FZ-α	SS#4.1_FY1-α

Camada 0 (Sensor e Atuador)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#1.1_FZ-α	A_FIS-N	A_FIS-N_1.2.2#2	Posicionador de válvula de controle
F-α	SS#1.1_FV-α	A_FIS-N	A_FIS-N_1.2.2#2	Válvula de controle

Camada 1 (Módulo ES)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY1-α	MIO_FIS-N	MIO_FIS-N_1.2.4#3	Cartão de entrada e saída

Camada 2 (Controlador)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY2-α	CNTR_FIS-N	CTR_FIS-N_1.2.4#4	Programador Lógico - PLC

Camada 3 (Supervisório)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	PC industrial
F-α	SS#4.1_ZI3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	Indicação virtual em Tela LCD - Posição da FV
F-α	SS#4.1_FI3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#6	Indicação virtual em Tela LCD - Status da FV
F-α	SS#4.1_HS3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#7	Indicação virtual em Tela LCD - Botoeira FV
F-α	SS#4.1_FY3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	PC industrial
F-α	SS#4.1_ZI3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	Indicação virtual em Tela LCD - Posição da FV
F-α	SS#4.1_FI3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#6	Indicação virtual em Tela LCD - Status da FV
F-α	SS#4.1_HS3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#7	Indicação virtual em Tela LCD - Botoeira FV

N_FV2
(Válvula de Controle de Vazão - Motorizada)

Interfaces de Dados

MALHA	LINK	TIPO	PROTOCOLO	DE	PARA
F-α	N#1.1.1	Digital	Ethernet	SS#4.1_FY2-α	SS#4.1_FY3a-α
F-α	N#1.2.1	Digital	Ethernet	SS#4.1_FY3a-α	SS#4.1_FY3b-α
F-α	N#2.1.1	Digital	Ethernet	SS#4.1_FY1-α	SS#4.1_FY2-α
F-α	N#3.1.1	Analógico	4-20mA	SS#1.1_FT-α	SS#4.1_FY1-α

Camada 0 (Sensor e Atuador)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FE-α	S_FIS-N	NA	Sensor de vazão
F-α	SS#4.1_FT-α	S_FIS-N	NA	Transmissor de pressão diferencial

Camada 1 (Módulo ES)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY1-α	MIO_FIS-N	MIO_FIS-N_1.2.4#3	Cartão de entrada e saída

Camada 2 (Controlador)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY2-α	CNTR_FIS-N	CTR_FIS-N_1.2.4#4	Programador Lógico - PLC

Camada 3 (Supervisório)

MALHA	TIPO	BTC	BTC#	Tecnologia/Informação
F-α	SS#4.1_FY3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	PC industrial
F-α	SS#4.1_ZI3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	Indicação virtual em Tela LCD - Posição da FV
F-α	SS#4.1_FI3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#6	Indicação virtual em Tela LCD - Status da FV
F-α	SS#4.1_HS3a-α	HSI_FIS-N	HSI_FIS-N_1.2.4#7	Indicação virtual em Tela LCD - Botoeira FV
F-α	SS#4.1_FY3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	PC industrial
F-α	SS#4.1_ZI3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#5	Indicação virtual em Tela LCD - Posição da FV
F-α	SS#4.1_FI3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#6	Indicação virtual em Tela LCD - Status da FV
F-α	SS#4.1_HS3b-α	HSI_FIS-N	HSI_FIS-N_1.2.4#7	Indicação virtual em Tela LCD - Botoeira FV

Fonte: Adaptado da simbologia e abreviações ISA 5.1.

3.c) Arquitetura típica e relatório ES - Alocação das Malhas de Controle

Na tabela 26 são apresentadas as funções declinadas para o nível 4 base para a alocação das malhas na tabela 27.

Tabela 26 - Exemplo de especificação de declinação de funções ativas

Nível 3					Nível 4							
Equipe	**Subsistema**		**Função de Serviço - FS# (FIS# + SS#)**		**Equipe**	**Subsistema**		**Função de Serviço - FS# (FIS# + SS#)**		**Bloco de Controle (Cod.FTC + FT#)**	**Camada de I&C**	**Agrupamento**
EPUNM #2	SS#2	Sistema do Primário	FIS-N_1.2.2	Prover auxiliares do Primário e Secundário	EPUNM #2.1	SS#2.1	Sistema de Auxiliares do SRR	FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	0	S_FIS-N
								FIS-N_1.2.2#2	Manipular o processo para Prover auxiliares do Primário e Secundário	A_FIS-N_1.2.2#2	0	A_FIS-N
			FIS-A_3.1.2	Controlar a reatividade	EPUNM #2.2	SS#2.2	Sistema de Refrigerante do Reator (SRR)	FIS-A_3.1.2#8	Medir o processo para Controlar a reatividade	S_FIS-A_3.1.2#8	0	S_FIS-A
								FIS-A_3.1.2#9	Manipular o processo para Controlar a reatividade	A_FIS-A_3.1.2#9	0	A_FIS-A
			FIS-A_3.2.2	Controlar o resfriamento do núcleo	EPUNM #2.3	SS#2.3	Sistema de Refrigerante do Reator (SRR)	FIS-A_3.2.2#1	Medir o processo para Controlar o resfriamento do núcleo	S_FIS-A_3.2.2#1	0	S_FIS-A
								FIS-A_3.2.2#2	Manipular o processo para Controlar o resfriamento do núcleo	A_FIS-A_3.2.2#2	0	A_FIS-A
			FIS-Q_1.2.1	Executar o SCRAM e ESFAS	EPUNM #2.4	SS#2.4	Sistema de Refrigerante do Reator (SRR)	FIS-Q_1.2.1#4	Medir o processo para Executar o SCRAM e ESFAS	S_FIS-Q_1.2.1#4	0	S_FIS-Q
								FIS-Q_1.2.1#5	Manipular o processo para Executar o SCRAM e ESFAS	A_FIS-Q_1.2.1#5	0	A_FIS-Q
			FIS-Q_1.2.2	Controlar o calor residual	EPUNM #2.5	SS#2.5	Sistema de Remoção de Calor Residual	FIS-Q_1.2.2#1	Medir o processo para Controlar o calor residual	S_FIS-Q_1.2.2#1	0	S_FIS-Q
								FIS-Q_1.2.2#2	Manipular o processo para Controlar o calor residual	A_FIS-Q_1.2.2#2	0	A_FIS-Q
			FIS-Q_2.1.2	Executar ESF	EPUNM #2.7	SS#2.7	Sistema de Remoção de Calor Residual	FIS-Q_2.1.2#1	Medir o processo para Executar ESF	S_FIS-Q_2.1.2#1	0	S_FIS-Q
								FIS-Q_2.1.2#2	Manipular o processo para Executar ESF	A_FIS-Q_2.1.2#2	0	A_FIS-Q

Na tabela 27 são apresentadas as alocações das malhas de controle conforme descrito no item 3.4.6.3. A sua concepção é em formato de matriz para permitir a alocação de cada bloco de controle (nível 4) a cada arquitetura típica elaborada para atender à UNM.

Tabela 27 - Exemplo de alocação das malhas de controle

Nível 4					**Lista do Catálogo de Arquiteturas Típicas de Controle**																							
					Medição de Vazão Simples	Medição de Vazão Dupla	Válvula de Controle de Vazão - Pneumática	Válvula de Controle de Vazão - Motorizada	Medição de Nível Simples	Medição de Nível Dupla	Válvula de Controle de Nível - Pneumática	Válvula de Controle de Nível - Motorizada	Medição de Vazão Simples	Medição de Vazão Dupla	Válvula de Controle de Vazão - Pneumática	Válvula de Controle de Vazão - Motorizada	Medição de Nível Simples	Medição de Nível Dupla	Válvula de Controle de Nível - Pneumática	Válvula de Controle de Nível - Motorizada	Medição de Temperatura Simples	Medição de Temperatura Dupla	Medição de Pressão Simples	Medição de Pressão Dupla	Válvula de Bloqueio - Pneumática	Válvula de Bloqueio - Motorizada	Bomba de circulação	Aquecedor	
Função de Serviço - FS# (FIS# + SS#)		**Bloco de Controle (Cod.FTC + FT#)**	**Camada de I&C**	**Agrupamento**	N_F1	N_F2	N_FV1	N_FV2	N_L1	N_L2	N_LV1	N_LV2	A_F1	A_F2	A_FV1	A_FV2	A_L1	A_L2	A_FL1	A_FL2	A_T1	A_T2	A_P1	A_P2	A_X1	A_X2	A_X1	A_X2	
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	0	S_FIS-N	F-001	F-002			L-001																				
FIS-N_1.2.2#2	Manipular o processo para Prover auxiliares do Primário e Secundário	A_FIS-N_1.2.2#2	0	A_FIS-N			FV-001					LV-001																	
FIS-A_3.1.2#8	Medir o processo para Controlar a reatividade	S_FIS-A_3.1.2#8	0	S_FIS-A									F-003				L-002					T-001	P-001	P-003					
FIS-A_3.1.2#9	Manipular o processo para Controlar a reatividade	A_FIS-A_3.1.2#9	0	A_FIS-A											FV-002					LV-002							X-003		
FIS-A_3.2.2#1	Medir o processo para Controlar o resfriamento do núcleo	S_FIS-A_3.2.2#1	0	S_FIS-A									F-004				L-003					T-002	P-002	P-004			X-004	X-005	
FIS-A_3.2.2#2	Manipular o processo para Controlar o resfriamento do núcleo	A_FIS-A_3.2.2#2	0	A_FIS-A																					X-001	X-002			

(...) Continua (...)

(...) Continua (...)

Notas:

(i). A tabela é apenas ilustrativa. Para simplificar, buscou-se colocar o símbolo "(...)"para indicar que há n itens a serem especificados para atender um projeto específico.

3.d) Arquitetura típica e relatório ES - Especificação dos Relatórios ES e FC

Na tabela 28 é apresentado o relatório de entradas e saídas de dados e das funções de controle conforme descrito no item 3.4.6.4. A sua concepção é em formato de matriz para permitir a relação de cada bloco de controle (nível 4) com seus links e tipos de sinais, a cada meio de controle da UNM.

Tabela 28 - Exemplo de relatórios ES e FC

Relatório ES

Função de Serviço - FS# (FIS# + SS#)		Bloco de Controle (Cod.FTC + FT#)	MALHA	TIPICO	LINK	PROCESSAMENTO	SINAL ANALÓGICO		SINAL DIGITAL		REDE		TIPO	PROTOCOLO	3	3	3	2	2	1	1	1
							EA	SA	ED	SD	ESCRITA	LEITURA			Cop_SCA#1	Etr_SCA#1A	Etr_SCA#1B	Rem_SCA#1A	Rem_SCA#1B	Mes_SCA#1A	Mes_SCA#1B	Mes_SCA#1C
															Sala de Controle	Sala de Controle	Elec. 2	Ger. Diesel 2	Ger. Diesel 1	SN.2	SN.2	SN.4
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-001	N_F1	N#1.1.1	SS#4.1_FY2-001					X		Digital	Ethernet				X	X			
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-001	N_F1	N#1.2.1	SS#4.1_FY3a-001					X		Digital	Ethernet	X							
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-001	N_F1	N#2.1.1	SS#4.1_FY1-001					X		Digital	Ethernet						X		
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-001	N_F1	N#1.1.1	SS#4.1_FY3a-001						X	Digital	Ethernet	X							
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-001	N_F1	N#1.2.1	SS#4.1_FY3b-001						X	Digital	Ethernet		X	X					
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-001	N_F1	N#2.1.1	SS#4.1_FY2-001						X	Digital	Ethernet				X	X			
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-001	N_F1	N#3.1.1	SS#4.1_FY1-001	X						Analógico	4-20mA + HART						X		
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-002	N_F2	N#1.1.1	SS#4.1_FY2-002					X		Digital	Ethernet				X	X			
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-002	N_F2	N#1.2.1	SS#4.1_FY3a-002					X		Digital	Ethernet	X							
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-002	N_F2	N#2.1.1	SS#4.1_FY1-002					X		Digital	Ethernet							X	
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-002	N_F2	N#1.1.1	SS#4.1_FY3a-002						X	Digital	Ethernet	X							
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-002	N_F2	N#1.2.1	SS#4.1_FY3b-002						X	Digital	Ethernet		X	X					
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-002	N_F2	N#2.1.1	SS#4.1_FY2-002						X	Digital	Ethernet				X	X			
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-002	N_F2	N#3.1.1	SS#4.1_FY1-002	X						Analógico	4-20mA + HART							X	
FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	S_FIS-N_1.2.2#1	F-002	N_F2	N#3.1.1	SS#4.1_FY1-002	X						Analógico	4-20mA + HART							X	

4) ESPECIFICAÇÃO DE SISTEMAS DE CONTROLE

4.a) Especificação de Sistemas de Controle – Descritivo do Sistema

1- Descritivo da hierarquia “top-down” e Funções de Serviço do Sistema de Controle

Na tabela 29 é apresentado um exemplo de especificação de declinação funcional (de cima para baixo) de sistemas de controle no nível 4 conforme descrito no item 3.4.7.1.

Tabela 29 - Exemplo de especificação - Declinação sistêmica

Sub-Sistema - Nível 3			Sub-Sistema - Nível 4		
Código	Descrição	Equipe	Código	Descrição	Equipe
SMC	Sistema de Monitoramento e Controle	ECUNM#1	SCA	Sistema de Controle Auxiliar	ECUNM#1.1
			SCR	Sistema de Controle do Reator	ECUNM#1.2
			SMI	Sistema de Monitoramento e Indicação (SMI)	ECUNM#1.3
SMP	Sistema de Monitoramento e Proteção	ECUNM#2	SMI	Sistema de Monitoramento e Indicação (SMI)	ECUNM#2.1
			SRT	Sistema de Proteção do Reator	ECUNM#2.2
			ESF	Sistema de Controle de Segurança	ECUNM#2.3

Na tabela 30 é apresentado um exemplo de especificação de funções de serviço de sistemas de controle no nível 4 conforme descrito no item 3.4.7.1.

Tabela 30 - Exemplo de especificação - Funções de Serviço

Cód. Função de Serviço	Correlação FIS	Descrição	Justificativa
(*Conforme a codificação utilizada no projeto*)	FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	Esta função ter por finalidade a inserção de sensores no processo para prover os parâmetros de processo para os sistemas de controle da UNM.
(*Conforme a codificação utilizada no projeto*)	FIS-N_1.2.2#2	Manipular o processo para Prover auxiliares do Primário e Secundário	Esta função ter por finalidade a inserção de atuadores para permitir que os sistemas de controle possam atuar no processo, manipulando as variáveis de processo da UNM.

(...) Continua (...)

2- Interfaces dos Sistema de Controle

Na tabela 31 é apresentado um exemplo de especificação de interfaces de sistemas de controle no nível 4 conforme descrito no item 3.4.7.1.

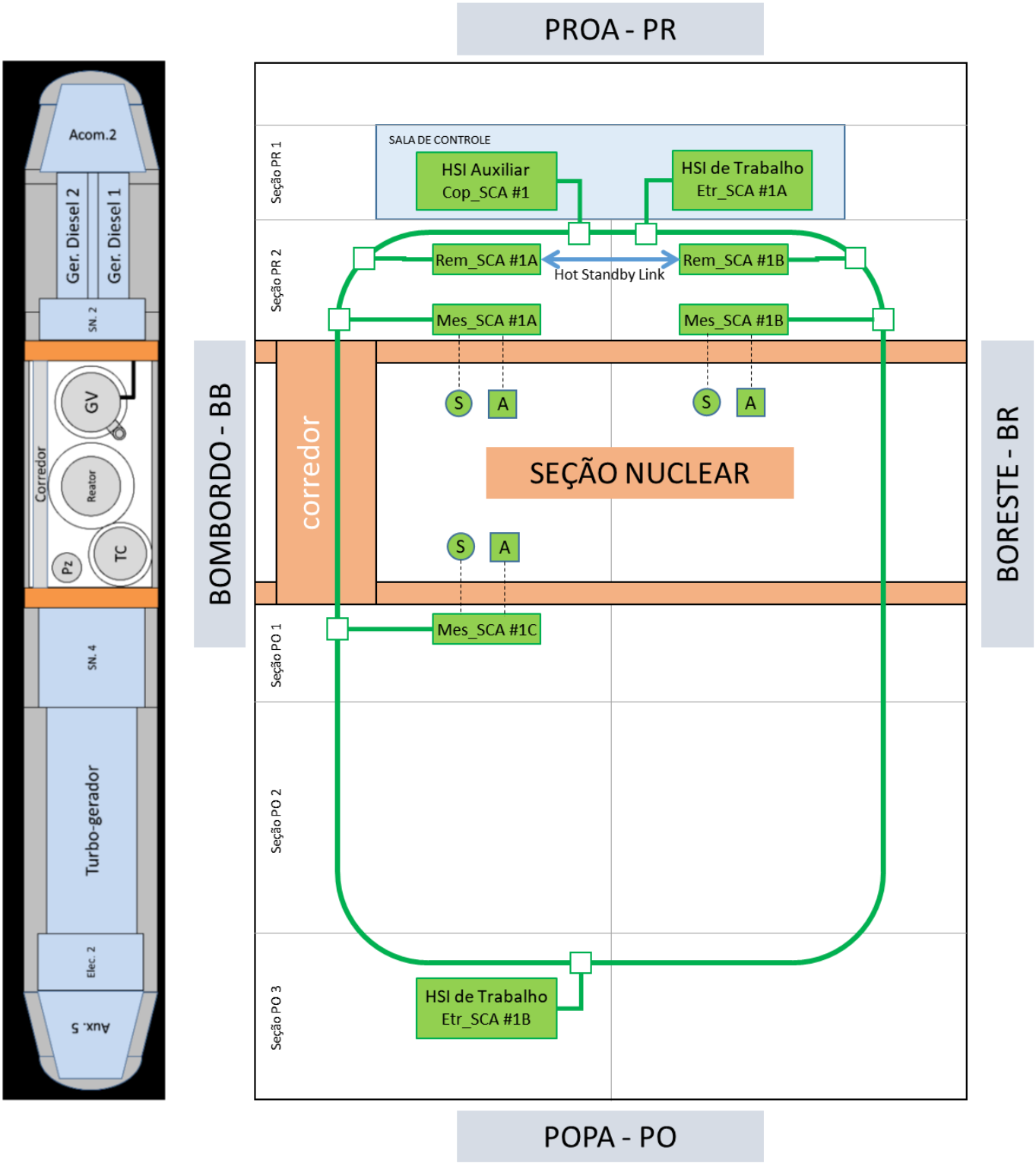
Tabela 31 - Exemplo de especificação - Interfaces

Requerente	Servidor	Tipo	Justificativa
Inserir o SS Nível 4 que necessita da Interface	Inserir o SS Nível 4 que provê a Interface	O tipo de interface pode ser do tipo: Elétrica; Fluida; Arranjo; Dados etc.	Na justificativa deve ser informada o porquê da necessidade, para qual propósito se precisa da interface, qual a necessidade, como deve ser providenciada a necessidade, e com quem será a interface.

3- Arquitetura Física Básica

Na figura 25 é apresentado um exemplo de arquitetura física de sistemas de controle no nível 4 conforme descrito no item 3.4.7.1.

Figura 25 - Exemplo de especificação - Arquitetura física básica

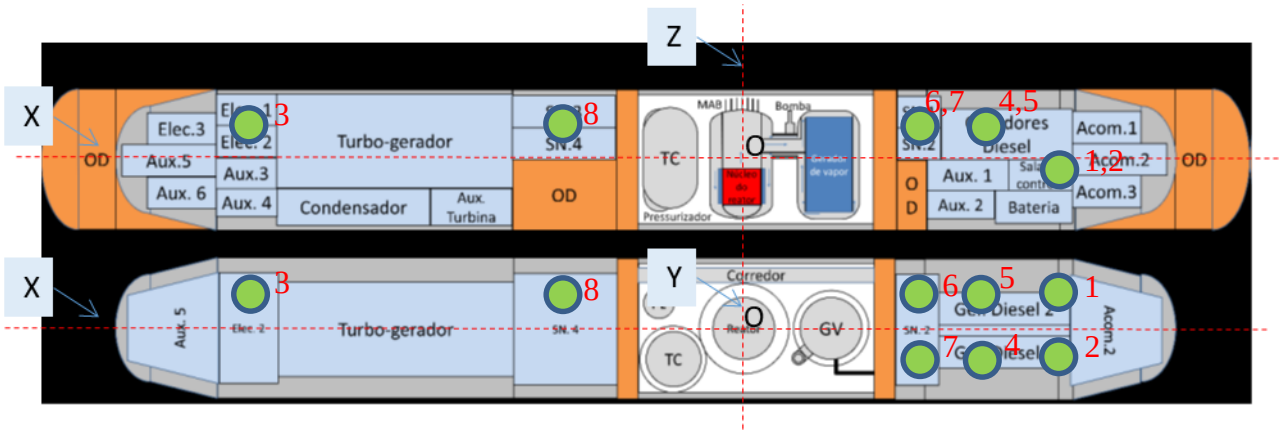


Fonte: adaptado de FREIRE (2018).

4- Arranjo dos equipamentos

Na figura 26 é apresentado um exemplo de arranjo de sistemas de controle conforme descrito no item 3.4.7.1.

Figura 26 - Exemplo de especificação – Arranjo geral da UNM



Fonte: Adaptado de FREIRE (2018)

Na tabela 32 é apresentado um exemplo de lista de localização dos equipamentos de sistemas de controle conforme descrito no item 3.4.7.1.

Tabela 32 - Exemplo de especificação - Arranjo dos equipamentos

Item	Equipmento	X	Y	Z	Compartmento
1	Cop_SCA#1	aa.bbb	-aa.bbb	-aa.bbb	Sala de Controle
2	Etr_SCA#1A	aa.bbb	aa.bbb	-aa.bbb	Sala de Controle
3	Etr_SCA#1B	-aa.bbb	-aa.bbb	-aa.bbb	Elec. 2
4	Rem_SCA#1 A	aa.bbb	-aa.bbb	aa.bbb	Ger. Diesel 2
5	Rem_SCA#1 B	aa.bbb	aa.bbb	aa.bbb	Ger. Diesel 1
6	Mes_SCA#1A	aa.bbb	-aa.bbb	aa.bbb	SN.2
7	Mes_SCA#1B	aa.bbb	aa.bbb	aa.bbb	SN.2
8	Mes_SCA#1C	-aa.bbb	-aa.bbb	aa.bbb	SN.4

5- Lista de equipamentos

Na tabela 33 é apresentado um exemplo de lista de equipamentos de sistemas de controle conforme descrito no item 3.4.7.1.

Tabela 33 - Exemplo de especificação - Lista de equipamentos

Item	Equipamento	Descrição	Mod.	Amb.	Compartimento	Crítico?	CSN
1	Cop_SCA#1	Consoles de operação do SCA	-	Ameno (Vante)	Sala de Controle	Sim	N
2	Etr_SCA#1A	Estações de trabalho do SCA	-	Ameno (Vante)	Sala de Controle	Não	N
3	Etr_SCA#1B	Estações de trabalho do SCA	-	Agressivo (Ré)	Elec. 2	Não	N
4	Rem_SCA#1A	Controle remoto do SCA	-	Ameno (Vante)	Ger. Diesel 2	Sim	N
5	Rem_SCA#1B	Controle remoto do SCA	-	Ameno (Vante)	Ger. Diesel 1	Sim	N
6	Mes_SCA#1A	Módulo ES do SCA	-	Ameno (Vante)	SN.2	Sim	N
7	Mes_SCA#1B	Módulo ES do SCA	-	Ameno (Vante)	SN.2	Sim	N
8	Mes_SCA#1C	Módulo ES do SCA	-	Agressivo (Ré)	SN.4	Sim	N

4.b) Especificação de Sistemas de Controle – Caracterização do Sistema

6- Características Funcionais

Na tabela 34 é apresentado um exemplo de lista de requisitos funcionais para sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 34 - Exemplo de especificação - Requisitos funcionais

Requisito#	Função impactada	Descrição	Flexibilidade
SCA_Func-1	FIS-N_1.2.2#1	Deve ser capaz de prover controle condições normais da UNM.	0
SCA_Func-2	FIS-N_1.2.2#1	Deve ser capaz de prover controle para “X” funções de controle.	1
SCA_Func-3	FIS-N_1.2.2#1	Deve ser capaz de prover controle para “X” sinais de entrada e saída analógicos.	0
SCA_Func-4	FIS-N_1.2.2#1	Deve ser capaz de prover controle para “X” sinais de entrada e saída digitais.	0
SCA_Func-5	FIS-N_1.2.2#1	Deve ser capaz de prover controle para “X” sinais escritos e lidos em rede de dados.	0
SCA_Func-6	FIS-N_1.2.2#1	Deve ser capaz de prover velocidade no trânsito de dados de “X”.	1
SCA_Func-7	FIS-N_1.2.2#1	Deve ser capaz de prover o tempo de resposta mínimo de “X”.	1

(...) Continua (...)

Notas:

Flexibilidade 0: Obrigatório (não há negociação em caso de desvio);
Flexibilidade 1: Negociável (deve ser apresentado o desvio para aprovação);
Flexibilidade 2: Desejável (o desvio deve ser apresentado para ciência do cliente); e
Flexibilidade 3: Opcional (o desvio não precisa ser claramente apresentado ao cliente).

7- Características dos Equipamentos

Na tabela 35 é apresentado um exemplo de lista de requisitos de equipamentos de sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 35 - Exemplo de especificação - Requisitos dos equipamentos

Requisito#	Equipamento impactado	Descrição	Flexibilidade
SCA_Equi-1	Cop_SCA#1	O console de operação deve ter no máximo as seguintes dimensões: aaa mm (larg.) x bbb mm (prof.) x ccc mm (altura).	0

Requisito#	Equipamento impactado	Descrição	Flexibilidade
SCA_ Equi - 2	Cop_SCA#1	O console de operação deve ter no máximo as seguinte peso: aaa kg.	1
SCA_ Equi - 3	Cop_SCA#1	O console de operação deve ter no máximo o seguinte consumo elétrico: aaa kg.	1
SCA_ Equi - 3	Cop_SCA#1	O console de operação deve ter no máximo a seguinte dissipação térmica: aaa kg.	1

(...) Continua (...)

8- Balanços

8.1 Balanço de peso

Na tabela 36 é apresentado um exemplo de balanço de peso para sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 36 - Exemplo de especificação - Balanço de peso

Equipamento	Descrição	Quantidade	Peso (Kg)
Cop_SCA#1	Consoles de operação do SCA	1	XX
Etr_SCA#1A	Estações de trabalho do SCA	1	XX
Etr_SCA#1B	Estações de trabalho do SCA	1	XX
Rem_SCA#1 A	Controle remoto do SCA	1	XX
Rem_SCA#1 B	Controle remoto do SCA	1	XX
Mes_SCA#1 A	Módulo ES do SCA	1	XX
Mes_SCA#1 B	Módulo ES do SCA	1	XX
Mes_SCA#1 C	Módulo ES do SCA	1	XX
Peso total dos equipamentos			YYY
Estimativa do peso de cabos			YYY
Estimativa do peso de suportes			YYY
Estimativa total			ZZZ

8.2 Balanço elétrico e térmico

Na tabela 37 é apresentado um exemplo de balanço elétrico e térmico para sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 37 - Exemplo de especificação - Balanço elétrico e térmico

Equipamento	Descrição	Quantidade	Consumo Elétrico (KW)	Dissipação Térmica (KW)
Cop_SCA#1	Consoles de operação do SCA	1	XX	XX
Etr_SCA#1A	Estações de trabalho do SCA	1	XX	XX
Etr_SCA#1B	Estações de trabalho do SCA	1	XX	XX
Rem_SCA#1 A	Controle remoto do SCA	1	XX	XX
Rem_SCA#1 B	Controle remoto do SCA	1	XX	XX
Mes_SCA#1 A	Módulo ES do SCA	1	XX	XX
Mes_SCA#1 B	Módulo ES do SCA	1	XX	XX
Mes_SCA#1 C	Módulo ES do SCA	1	XX	XX
Estimativa total			ZZZ	ZZZ

9- Característica Não Funcionais

9.1 Segurança Não Nuclear

Na tabela 38 é apresentado um exemplo de lista de requisitos de segurança não nuclear para sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 38 - Exemplo de especificação - Requisitos de SNN

Requisito	Descrição	Flexibilidade
SS#-SNN-1	[prever requisitos referente a detecção e combate a fogo]	1
SS#-SNN-2	[prever requisitos referente a penetrações em anteparas não nucleares do navio, com critérios de estanqueidade, isolamento elétrico, aterramento etc.]	1
SS#-SNN-3	[prever requisitos referente à segurança cibernética]	1
SS#-SNN-4	[prever requisitos referente a agressões externas: vazamento de vapor, radiação, alagamento etc.]	1
SS#-SNN-5	[prever requisitos referente a condições ambientais no navio]	1

9.2 Segurança Nuclear

Na tabela 39 é apresentado um exemplo de lista de requisitos de segurança nuclear para sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 39 - Exemplo de especificação - Requisitos de SNU

Requisito	Descrição	Flexibilidade
SS#-SNU-1	[prever requisitos referente a qualidade (declinação dos requisitos do GDC 1): ASME NQA-1 ou ISO 9001.]	1
SS#-SNU-2	[prever requisitos referente a categoria sísmica (declinação dos requisitos do GDC 2).]	1
SS#-SNU-3	[prever requisitos referente a localização de equipamentos ou proteções físicas para minimizar danos decorrentes de incêndios (declinação dos requisitos do GDC 3).]	1
SS#-SNU-4	[prever requisitos referente a resistência a eventos agressivos ou degradantes (declinação dos requisitos do GDC 4).]	1

9.3 Restrições de projeto

Na tabela 40 é apresentado um exemplo de lista de requisitos de projeto para sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 40 - Exemplo de especificação - Requisitos de PRO

Requisito	Descrição	Flexibilidade
SS#-PRO -1	[prever requisitos referente a conforto acústico.]	1
SS#-PRO -2	[prever requisitos referente a choque e vibração.]	1
SS#-PRO -3	[prever requisitos referente a compatibilidade eletromagnética.]	1

9.4 Construtabilidade, mantenabilidade e logística

Na tabela 41 é apresentado um exemplo de lista de requisitos de construtibilidade, mantenibilidade e logística para sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 41 - Exemplo de especificação - Requisitos de CML

Requisito	Descrição	Flexibilidade
SS#-CML-1	[prever requisitos referente ao ciclo de vida do empreendimento, plano de obsolescência e descomissionamento.]	0
SS#-CML-2	[prever requisitos referente ao ciclos de parada para manutenção geral.]	0

Requisito	Descrição	Flexibilidade
SS#-CML-3	[prever requisitos referente estratégias de manutenção preventiva e preditiva.]	1
SS#-CML-4	[prever requisitos referente critérios de desempenho para funções relevantes para a missão.]	1
SS#-CML-5	[prever requisitos referente a dimensões necessárias para desmontagem e transporte de peças e componentes durante construção ou manutenção.]	0

9.5 Normas de segurança do trabalho e qualidade

Na tabela 42 é apresentado um exemplo de lista de requisitos de segurança do trabalho e qualidade para sistemas de controle conforme descrito no item 3.4.7.2.

Tabela 42 - Exemplo de especificação - Requisitos de STQ

Requisito	Descrição	Flexibilidade
SS#-STQ-1	[prever requisitos referente à base normativa.]	0
SS#-STQ-2	[prever requisitos referente a normas de segurança de elétrica.]	0
SS#-STQ-3	[prever requisitos referente a necessidade de manuais que facilitem a leitura de itens sobre a segurança do uso e manuseio do equipamento pelo operador.]	0
SS#-STQ-4	[prever requisitos referente a proibição de uso de materiais combustíveis.]	0

4.c) Especificação de Sistemas de Controle – Operação do Sistema

10- Diagrama de estados e transições

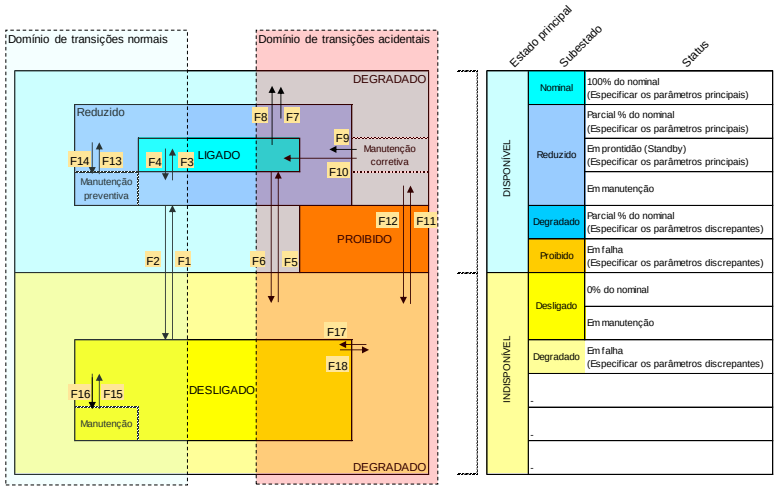
Na tabela 43 é apresentado um exemplo de lista de funções e estados para sistemas de controle conforme descrito no item 3.4.7.3. A figura 27 apresenta um diagrama de estados genérico que pode ser utilizado como referência para a elaboração da tabela 43.

Tabela 43 - Exemplo de especificação - Função e estados da UNM

Cód. Função de Serviço	Correlação FIS	Descrição	UNM Disponível		UNM Indisponível					
			Nominal ou Reduzido	Reduzido	Parado			Degradado		
			UNM_em_potência	UNM_em_prontidão	UNM_em_hotshutdown	UNM_em_coldshutdown	UNM_em_longotermo	UNM_em_safeshutdown	UNM_em_LOCA	UNM_em_ATWS
(Conforme codificação do projeto)	FIS-N_1.2.2#1	Medir o processo para Prover auxiliares do Primário e Secundário	Relevante	Relevante	Irrelevante	Irrelevante	Irrelevante	Irrelevante	Irrelevante	Irrelevante

(...) Continua (...)

Figura 27 - Diagrama de estados



Fonte: adaptado de FREIRE (2018).

Na tabela 44 é apresentado um exemplo de lista de descrição de fases para sistemas de controle conforme descrito no item 3.4.7.3.

Tabela 44 - Exemplo de especificação - Descrição das fases

Fase	Descrição
F1	Esta fase implica na inicialização do Sistema de Controle, que ainda se encontra no estado de desempenho reduzido.
F2	Esta fase implica no desligamento do Sistema de Controle.
F3	O Sistema atinge o desempenho esperado, e vai para a condição nominal.
F4	O sistema é retirado do regime nominal e é reduzido em seu desempenho.

(...) Continua (...)

11- Descritivo de operação

Os modelos de especificação de operação do sistema encontram-se nas tabelas 22 e 23 do item 3.a.

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Diretoria de Pesquisa, Desenvolvimento e Ensino
Av. Prof. Lineu Prestes, 2242 – Cidade Universitária CEP: 05508-000
Fone/Fax(0XX11) 3133-8908
SÃO PAULO – São Paulo – Brasil
http://www.ipen.br

O IPEN é uma Autarquia vinculada à Secretaria de Desenvolvimento, associada à Universidade de São Paulo e gerida técnica e administrativamente pela Comissão Nacional de Energia Nuclear, órgão do Ministério da Ciência, Tecnologia, Inovações e Comunicações.